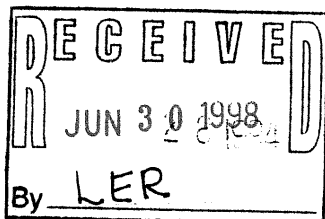


**ORDER**

**DOCUMENTATION CONTROL CENTER**

1600.6C

**PHYSICAL SECURITY MANAGEMENT PROGRAM**



**AUA TAC  
DOCUMENT MANAGEMENT  
CENTER**



**April 16, 1993**

**U.S. DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION**

Distribution: A-WXYZ-3; A-FCS-O (LTD) A-FOF-O (LTD)

Initiated By: ACP-120

**LIBRARY USE ONLY**

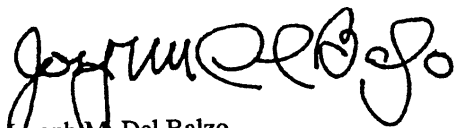
## FOREWORD

This order assigns responsibilities, delegates authority, and prescribes standards and procedures for the Federal Aviation Administration (FAA) Physical Security Management Program (PSMP).

It establishes procedures to ensure compliance with applicable Public Laws, national security directives and policies, and Department of Transportation (DOT) orders. It also directs the Assistant Administrator for Civil Aviation Security, ACS-1, to exercise on behalf of the Administrator overall responsibility and authority for the FAA PSMP, and to promulgate necessary operational standards and procedures to manage the program through the Office of Policy and Planning, Policy and Standards Division, ACP-100.

In order for the FAA to ensure that its facilities are ready to perform their vital functions in support of the National Airspace System, it is the responsibility of every manager and employee to ensure that they comply with the policies, standards, and procedures contained in this directive.

This order establishes the Facility Inspection Reporting Subsystem (FIRS) as the primary means of reporting, screening, and processing physical security inspection data for the FAA.



Joseph M. Del Balzo  
Acting Administrator

# TABLE OF CONTENTS

Page

## CHAPTER 1. GENERAL

1. Purpose.....	1
2. Distribution.....	1
3. Cancellation .....	1
4. Background.....	1
5. Explanation of Changes.....	1
6. Definitions .....	1
7. Authority to Change this Order .....	1
8. Forms and Reports.....	2
9. Requests for Information.....	2
10. Other FAA Standards and Directives .....	2
11. Policy .....	2
12. Scope.....	2
13. Responsibilities of Regional Administrators, Associate Administrator of Aeronautical Center, and Director of Technical Center.....	2
14. Responsibilities of Assistant Administrator for Information Technology, AIT-1.....	2
15. Responsibilities of the Assistant Administrator for Civil Aviation Security.....	2
16. Responsibilities of the Director, Office of CAS Policy and Planning, ACP-1.....	2
17. Responsibilities of the Director, Office of CAS Operations, ACO-1.....	2
18. Responsibilities of the Manager, Investigations and Security Division, Operations, ACO-300 .....	3
19. Responsibilities of Managers, Civil Aviation Security Divisions, and Staffs .....	3
20. Responsibilities of the Office of Director, National Airspace System (NAS) Systems Engineering Service .....	3
21. Responsibilities of the Office of Director, Air Traffic System Management.....	3
22. Responsibilities of the Office of Director, Air Traffic Plans and Requirements Service.....	3
23. Responsibilities of the Office of Director, NAS Transition and Implementation Service .....	3
24. Responsibilities of the Office of Director, Systems Maintenance Service .....	4
25. Responsibilities of the Associate Administrator for Contracting and Quality Assurance, ASU-1 .....	4
26. Responsibilities of Regional Program and Project Managers.....	4
27. Responsibilities of FAA Facility Managers .....	4
28. Responsibilities of FAA and Contractor Employees .....	4
29.-199. Reserved.....	4

## CHAPTER 2. PHYSICAL SECURITY EVALUATION

200. Objective.....	9
201. Accreditation/Evaluation .....	9
202. Accreditation/Evaluation Approval.....	9
203. Accreditation/Evaluation Scheduling.....	9
204. Follow Up Procedures .....	9
205. Changes Affecting Physical Security Evaluation.....	9
206.-299. Reserved.....	9

**CHAPTER 3. FACILITY PLANNING AND DESIGN****SECTION 1. GENERAL**

300. Objective .....	15
301. Responsibilities of the Servicing Security Element (SSE) .....	15
302. Responsibilities of the Program/Project Manager .....	15
303. New Facilities, Office Spaces, and Operating Areas .....	15
304. Redesigning Existing Facilities .....	15
305. Commercially Leased Space .....	15
306.-310. Reserved .....	16

**SECTION 2. PLANNING AND DESIGN**

311. Personnel Entrances .....	16
312. Safety and Fire Protection .....	16
313. Utilities .....	17
314. Organizational Layout .....	17
315.-322. Reserved .....	17

**SECTION 3. EMERGENCY AND CONTINGENCY PLANNING**

323. General .....	17
324. Emergency Operations Plan .....	17
325. Contingency Plan .....	17
326. Occupant Emergency Plan (OEP) .....	17
327. Responsibility .....	18
328. FAA Offices and Facilities .....	18
329. FAA Offices in GSA Controlled Facilities .....	18
330. FAA-Leased Space .....	18
331. Initiating Action Under the OEP .....	18
332. Terrorist Demands, Threats, or Actions .....	18
333. Relationship to the PSMP .....	18
334. Bomb Threats .....	19
335. Civil Disturbances .....	19
336. Testing of OEP .....	19
337.-399. Reserved .....	19

**CHAPTER 4. PHYSICAL SECURITY RISK ANALYSIS**

400. Objective .....	25
401. Relationship to the PSMP .....	25
402. Criticality .....	25
403. Replacement .....	25
404. Concept of Risk .....	25
405. Physical Security Threats .....	25
406. Terrorist Threat to FAA Facilities .....	25
407. Obtaining Threat Information .....	25
408. Countermeasures .....	25
409.-499. Reserved .....	25



**CHAPTER 5. FAA FACILITY SECURITY STANDARDS PERIMETER AND EXTERIOR CONTROLS**

500. Objective.....	31
501. Approach.....	31

**SECTION 1. PERIMETER BARRIERS**

502. Perimeter Controls.....	31
503. Purpose of Perimeter Barriers.....	31
504. FAA Standard Security Fence.....	31
505. Clear Zone.....	31
506. When the Clear Zone Requirement Cannot be Met.....	31
507. Grounding.....	31
508. Construction.....	32
509. Gate Entrances.....	32
510. Unattended Gates.....	32
511. Semi-Active Gates.....	32
512. Gate Construction.....	32
513. Perimeter Warning Signs.....	32
514. Protection in Depth.....	32
515. Alternative Barriers.....	32

**SECTION 2. PROTECTIVE LIGHTING**

516. Objectives.....	32
517. Design Standards.....	32
518. Application.....	33
519. Active Entrances.....	33
520. Semi-Active and Inactive Perimeter Entrances.....	33
521. Critical Assets.....	33
522. Parking Lot Areas.....	33
523. Security Guard Gate House.....	33
524. Emergency Power.....	33

**SECTION 3. VEHICLE AND PARKING CONTROL**

525. Selection of Parking Areas.....	33
526. Parking Area Requirements.....	33
527. Guard Monitoring.....	33
528. Visitor Parking.....	33

**SECTION 4. PERIMETER IDS**

529. Perimeter Intrusion Detection System (PIDS).....	33
---	----

**SECTION 5. BUILDING CONTROLS**

530. General.....	34
531. Doors.....	34
532. Number of Entrances.....	34
533. Construction.....	34
534. Windows.....	34
535. Security Concerns.....	34

536. Window Construction .....	34
537. Miscellaneous Openings .....	34
538. Requirement .....	34
539. Safeguards for Miscellaneous Openings .....	34
540. Fire Escapes .....	34
541. Walls .....	35
542. Wall Safeguards .....	35
543.-550. Reserved. ....	35

## SECTION 6. GUARD FORCE

551. Objective .....	35
552. Determination of Need .....	35
553. Contract Guard Requirements .....	35
554.-599. Reserved. ....	36

## CHAPTER 6. FAA FACILITY SECURITY STANDARDS INTERIOR AND ASSET CONTROLS

### SECTION 1. CRITICAL AREAS

600. General .....	41
601. Criteria for the Designation of Critical Areas .....	41
602. Controlling Critical Areas .....	42
603. Locking Devices .....	42
604. Issuance and Control of Locks and Keys .....	42

### SECTION 2. SAFEGUARDING GOVERNMENT FUNDS

605. Protection of Government Funds .....	43
606. SSE Responsibilities .....	43
607. Safeguarding Concerns .....	43
608. Fund Storage Rooms .....	43

### SECTION 3. SAFEGUARDING GOVERNMENT PROPERTY

609. Small Arms and Ammunition Storage and Protection .....	43
610. Protection of Government Property .....	43
611. Theft Targets .....	44
612. Shipping and Receiving Operations .....	44
613. Loan Pools .....	44
614. General and Specialized Storage Areas .....	44
615. For Remote Storage Areas .....	44
616. Other FAA Storage Areas .....	44

### SECTION 4. THEFT PREVENTION

617. Theft Prevention Measures .....	45
618. Property Management System .....	45
619. Accountable Equipment Categories .....	46
620. Removal of Property from FAA Facilities .....	46
621. In Buildings Where FAA is the Sole or Primary Tenant .....	46
622. In Buildings Where Entry and Exit Are Not Subject to Guard Supervision .....	46
623. Property Removal Requirements .....	46

624. When Verification of Authority to Remove Property From an FAA Facility Cannot Be Obtained .....	47
625. Physical Protection of Office Equipment .....	47
626-631. Reserved .....	47

## SECTION 5. ASSET CONTROLS

632. Destruction Equipment .....	47
633. Storage Equipment .....	48
634. Vaults and Strongrooms .....	48
635-699. Reserved .....	48

## CHAPTER 7. FACILITY PHYSICAL SECURITY MANAGEMENT PLAN (FPSMP)

700. Objective .....	53
701. Responsibilities .....	53
702. Applicability .....	53
703. Planning Considerations .....	53
704. Developing the FPSMP .....	54
705. Indicators .....	54
706. Planning Goals .....	54
707. FPSMP Format .....	54
708-799. Reserved .....	54

## CHAPTER 8. SURVEYS AND INSPECTIONS

800. Purpose .....	59
801. Establishing Priorities .....	59
802. Program Management .....	59
803. Servicing Security Element (SSE) .....	59

### SECTION 1. SURVEYS

804. Description .....	59
805. Initial Surveys .....	59
806. Evaluation Surveys .....	59
807. Supplemental Surveys .....	59
808. Special Surveys .....	59

### SECTION 2. CONDUCT OF SECURITY SURVEYS

809. Procedures .....	59
810. Program Evaluation .....	59
811. Survey Coordinator .....	60
812. Initial Planning .....	60
813. Contents .....	60
814. Survey Team Members .....	60
815. Survey Reports .....	60

### SECTION 3. INSPECTIONS

816. Description .....	60
817. Comprehensive Inspections .....	60
818. Supplemental Inspections .....	60

819. Special Inspections .....	60
--------------------------------	----

#### **SECTION 4. CONDUCT OF INSPECTIONS**

820. Preparation .....	60
821. Entrance Briefing .....	60
822. Exit Briefing .....	60
823. Facility Inspection Reporting Subsystem (FIRS) .....	61
824. General .....	61
825. Follow-up Reports .....	61
826.-899. Reserved .....	61

#### **APPENDIX 1. GLOSSARY OF TERMS ( 3 Pages)**

#### **APPENDIX 2. OTHER STANDARDS, LAWS, DIRECTIVES, AND ORDERS THAT APPLY TO THE SAFEGUARDING OF FAA FACILITIES AND ASSETS UNDER THE PHYSICAL SECURITY MANAGEMENT PLAN (2 Pages)**

#### **APPENDIX 3. FORMS AND REPORTS (3 Pages)**

#### **APPENDIX 4. OCCUPANT EMERGENCY PLAN - SAMPLE FORMAT (18 Pages)**

#### **APPENDIX 5. PERIMETER CONTROLS ( 3 Pages)**

#### **APPENDIX 6. LIGHTING (4 Pages)**

#### **APPENDIX 7. BUILDING CONTROLS (3 Pages)**

#### **APPENDIX 8. SECURITY GUARD FORCE (6 Pages)**

#### **APPENDIX 9. KEY AND LOCK CONTROL PROCEDURES (1 Pages)**

#### **APPENDIX 10. SAFEGUARDING GOVERNMENT FUNDS (2 Pages)**

#### **APPENDIX 11. STANDARDS FOR THE SAFEGUARDING AND USE OF FIREARMS AND CHEMICAL IRRITANTS (8 Pages)**

#### **APPENDIX 12. STORAGE CONTAINERS, VAULTS, AND STRONGROOMS (3 Pages)**

#### **APPENDIX 13. TYPES OF FAA FACILITIES (2 Pages)**

#### **APPENDIX 14. FACILITY PHYSICAL SECURITY MANAGEMENT PLAN (3 Pages)**

#### **APPENDIX 15. SECURITY SURVEY PROCEDURES (1 Page)**

#### **APPENDIX 16. ACCREDITATION EVALUATION CERTIFICATION (1 Page)**

#### **APPENDIX 17. FACILITY INSPECTION REPORTING SUBSYSTEM (FIRS) (3 Pages)**

## CHAPTER 1. GENERAL

**1. PURPOSE.** This order establishes the Federal Aviation Administration (FAA) Physical Security Management Program (PSMP). It establishes physical security accreditation for all FAA facilities as a major objective and establishes standards for physical security management, control, and safeguarding of assets and facilities. It provides for the conduct of risk analyses, surveys, and inspections to identify countermeasures and ensure the effectiveness of the program. This order also implements Order DOT 1660.1, Removal of Equipment from DOT Buildings; Order DOT 1600.23, Demonstrations in or Near Government Buildings; Order DOT 1600.26A, Department of Transportation Physical Security Program; Order DOT 1620.1, Use of Weapons by DOT Personnel; Order DOT 1620.3, Policy on Departmental Employees Carrying Weapons Aboard Commercial Aircraft; Order DOT 1620.4, Possession of Privately Owned Firearms in or on DOT Owned or Leased Property; and Order DOT 1660.4, Physical Security Review of New Facilities, Office Space, or Operating Areas.

**2. DISTRIBUTION.** This order is distributed to branch level in the Washington headquarters, regions, and centers and to Civil Aviation Security Field Offices (CASFO), with a limited distribution to other field offices and facilities.

**3. CANCELLATION.** The following orders are canceled:

a. Order 1600.6B, Protection of Agency Property, dated August 25, 1978.

b. Order 1600.39, Removal of Equipment from Department of Transportation Buildings, dated November 14, 1974.

c. Order 1600.46, Physical Security Review of New Facilities, Office Space or Operating Areas, dated July 14, 1975.

d. Order 1600.53, Safeguarding and Use of Firearms, dated February 10, 1977.

**4. BACKGROUND.** Physical security management and the application of appropriate physical security controls at FAA facilities are essential elements in eliminating or reducing to a reasonable level the risk of fraud, waste and abuse, and the risks resulting from espionage, sabotage, theft, malicious mischief, terrorism, or other criminal acts causing loss or damage to U.S. Government property, injury to FAA employees, or loss or impairment of the capability of FAA facilities to perform critical air safety functions in their mission of supporting the National Airspace System (NAS). The success of the PSMP requires the cooperation and support of management at all levels in working with the appropriate servicing security element (SSE) to establish physical

security and risk reduction programs that are appropriate for the specific needs of each facility. It is also important that this cooperation begin as early in the planning and development of new facilities as possible. The most effective security system development will ensure that security measures are integrated and complement each other to achieve the desired objective. Through the accreditation process, and the survey and inspection program of the PSMP, it will be possible to monitor the effectiveness of the program and to ensure that its objectives are achieved.

### 5. EXPLANATION OF CHANGES.

a. The title of the program has been changed from Protection of Agency Property to Physical Security Management Program (PSMP).

b. Physical security standards and criteria have been expanded and made applicable to assets and facilities agencywide.

c. The accreditation process is established as a principal objective of the PSMP.

d. The responsibilities of offices, services, and field elements in support of the PSMP have been expanded.

e. Servicing security element (SSE) is used throughout the document to refer to the Civil Aviation Security Divisions (CASD) and the Technical Center Security Staff.

f. Risk analysis is established as a standard procedure to aid in determination of safeguarding requirements and countermeasures.

g. The Facility Inspection Reporting Subsystem (FIRS) is established as the standard for the collection and reporting of the results of PSMP inspections.

h. Security survey standards and procedures have been expanded.

i. Reference orders have been listed by their number without the edition suffix. (i.e. 1600.6, instead of 1600.6B).

j. Physical security safeguarding requirements established by other FAA orders and directives are recognized in this order as the applicable standards for the areas to which they pertain.

**6. DEFINITIONS.** Appendix 1, Glossary of Terms, contains definitions of terms used in this directive.

**7. AUTHORITY TO CHANGE THIS ORDER.** The Assistant Administrator for Civil Aviation Security may issue changes to this order necessary to implement and manage the

PSMP. The Administrator reserves the authority to approve changes which establish policy, delegate authority, or assign responsibility.

**8. FORMS AND REPORTS.** Information concerning the forms and reports addressed in this order is contained in paragraphs 623a, 815, 824, 825, and Appendices 3 and 17.

**9. REQUESTS FOR INFORMATION.** Requests for information concerning this directive should be addressed to the servicing security element in regions and centers. In Washington headquarters, requests should be addressed to ACP-120.

**10. OTHER FAA STANDARDS AND DIRECTIVES.** Physical security safeguarding standards and requirements contained in other FAA orders and directives, as well as those applicable requirements specified in Public Law and national policy, are applicable to the PSMP. Appendix 2 contains a partial listing of other FAA standards, Public Laws, and national policy documents that apply to the requirements of the PSMP.

**11. POLICY.** This order prescribes the policy of the FAA that management at all levels shall work with the appropriate SSE representatives to ensure that personnel and physical security management and control safeguards contained in this directive are applied at all FAA facilities. Security management procedures, controls, and safeguards shall be applied to the extent that is necessary to eliminate or reduce identified vulnerabilities to achieve an acceptable level of risk. An acceptable level of risk is one that, based on all available information, is determined to meet the goals of the PSMP with regard to a specific facility. This determination is made by the SSE in coordination with the facility manager based upon the provision of reasonable safeguards for FAA personnel, assets and operations from criminal acts, and other physical security risks and threats. When measures to reduce existing vulnerabilities cannot be accomplished because of physical, operational, or resource limitations, waivers may be considered. Requests for waivers or exceptions shall be addressed through regional SSE. Copies of each waiver granted by the SSE shall be sent to ACO-320. All requests for exceptions to policy shall be forwarded through the appropriate regional SSE to ACP-120.

**12. SCOPE.** This order applies to all FAA employees, contractor employees working for the FAA or in FAA facilities, and military personnel assigned to the FAA; it includes facilities and offices of the FAA having responsibility for the control, movement, storage, maintenance, and/or physical security of personnel, material, equipment, and documents. FAA operations that are housed within a public building under control of the General Services Administration (GSA) are also subject to applicable requirements of GSA Public Building Service Regulation P5930.17A.

### **13. RESPONSIBILITIES OF REGIONAL ADMINISTRATORS, ASSOCIATE ADMINISTRATOR OF AERONAUTICAL CENTER, AND DIRECTOR OF TECHNICAL CENTER are:**

a. Implementing the requirements of this directive in those offices under their respective jurisdictions.

b. Ensuring that procedures are in place to coordinate security requirements for the development of programs and projects for construction of new facilities and/or modification of existing facilities with the appropriate SSE.

**14. RESPONSIBILITIES OF ASSISTANT ADMINISTRATOR FOR INFORMATION TECHNOLOGY, AIT-1.** The Assistant Administrator for Information Technology in coordination with the Assistant Administrator for Civil Aviation Security, ACS-1, is responsible for the development of FAA automated systems, security policies, and standards.

**15. RESPONSIBILITIES OF THE ASSISTANT ADMINISTRATOR FOR CIVIL AVIATION SECURITY.** The Assistant Administrator for Civil Aviation Security, on behalf of the Administrator, exercises overall responsibility and authority for the FAA physical security programs and, through the Directors, Office of Civil Aviation Security (CAS), Operations, ACO-1, and Office of CAS Policy and Planning, ACP-1, takes necessary management actions to ensure that the Administration's interests are effectively protected.

**16. RESPONSIBILITIES OF THE DIRECTOR, OFFICE OF CAS POLICY AND PLANNING, ACP-1.** The Director, Office of CAS Policy and Planning, ACP-1, is responsible for:

a. Coordinating with ACO-1 in assessing the need for new or revised PSMP policy.

b. Developing new policies required to support identified needs of the PSMP.

c. Determining the need for and recommending PSMP related research and development projects to the Scientific Advisor, ACS-20.

**17. RESPONSIBILITIES OF THE DIRECTOR, OFFICE OF CAS OPERATIONS, ACO-1.** The Director, Office of CAS Operations, ACO-1, is responsible for:

a. Implementing agency policy pertaining to the PSMP.

b. Ensuring the effectiveness of the PSMP through assessments, evaluations, surveys, inspections, and security education.

c. Coordinating with ACP-1 the results of assessments and evaluations to determine the need for new or modified PSMP policies and procedures.

d. Providing budget and personnel resources required to fully support the PSMP.

**18. RESPONSIBILITIES OF THE MANAGER, INVESTIGATIONS AND SECURITY DIVISION, OPERATIONS, ACO-300.** The Manager, Investigations and Security Division, ACO-300, is responsible for:

a. Ensuring that action is taken to address significant physical security vulnerabilities or unacceptable physical security risks to the national security, the FAA, and the NAS.

b. Reviewing the PSMP reports submitted to ACO-1 for content, accuracy, and assessment of corrective actions taken.

c. Ensuring that accreditation and physical security surveys and inspections are conducted of critical FAA facilities.

d. Providing technical leadership in physical security system implementation.

e. Ensuring that statistical and reporting requirements imposed by DOT are met.

**19. RESPONSIBILITIES OF MANAGERS, CIVIL AVIATION SECURITY DIVISIONS AND STAFFS.** Managers of Civil Aviation Security Divisions, -700's, and Civil Aviation Security Staff, ACT-8, are responsible for:

a. Implementing the provisions of this order within their respective areas of jurisdiction.

b. Ensuring that staffing standards are developed to accurately reflect the number of physical security specialist positions required to implement the provisions of the PSMP.

c. Coordinating with region/center program and project managers in reviewing requirements for new construction and office space to ensure that standards established by this order are included in the program or project.

d. Monitoring compliance with the PSMP through a comprehensive program of physical security surveys and inspections.

e. Ensuring that appropriate follow-up action is taken to support facility managers in resolving deficiencies identified during the conduct of surveys and inspections.

**20. RESPONSIBILITIES OF THE OFFICE OF DIRECTOR, NATIONAL AIRSPACE SYSTEM (NAS) SYSTEMS ENGINEERING SERVICE.** The Office of the Director, NAS Systems Engineering Service, ASE-1, is responsible for formulating guidance and standards applicable to the acquisition of security systems and equipment.

**21. RESPONSIBILITIES OF THE OFFICE OF DIRECTOR, AIR TRAFFIC SYSTEM MANAGEMENT.** The Office of the Director, Air Traffic System Management, ATM-1, is responsible for:

a. Implementing the requirements of this order.

b. Ensuring that the requirements of this order are implemented by all ATM subordinate offices and activities.

c. Coordinating with the Office of Director, CAS Operations, ACO-1, to identify and implement physical security safeguarding requirements for critical air traffic control (ATC) facilities, equipments, and operations in accordance with requirements of this order.

**22. RESPONSIBILITIES OF THE OFFICE OF DIRECTOR, AIR TRAFFIC PLANS AND REQUIREMENTS SERVICE.** The Office of the Director, Air Traffic Plans and Requirements Service, ATR-1, is responsible for:

a. Coordinating with Director of CAS Operations, ACO-1, to identify and implement procedures and standards for the physical security safeguarding of FAA facilities in the ATC system.

b. Serving as the Air Traffic (AT) focal point for coordination and implementation of PSMP standards and requirements within the AT system.

**23. RESPONSIBILITIES OF THE OFFICE OF DIRECTOR, NAS TRANSITION AND IMPLEMENTATION SERVICE.** The Office of Director, NAS Transition and Implementation Service, ANS-1, is responsible for:

a. Coordinating with Director of CAS Operations, ACO-1, in the engineering, acquisition, and implementation of physical security systems and requirements contained in this order.

b. Coordinating with the directors of the offices of CAS Operations, ACO-1, Systems Maintenance, ASM-1, and Program and Resource Management, ACZ-1, in the identification of required maintenance training for support of installed security systems.

**24. RESPONSIBILITIES OF THE OFFICE OF DIRECTOR, SYSTEMS MAINTENANCE SERVICE.** The Office of the Director, Systems Maintenance Service, ASM, is responsible for:

a. **Identifying maintenance requirements** in coordination with the Office of Director, CAS Operations, ACO-1, for the incorporation of physical security requirements of this order in plans for new facilities as well as in plans for modifying existing facilities.

b. **Coordinating** with the Office of Civil Aviation Security Program Management, ACZ-1, in the development of required physical security system maintenance training for FAA personnel.

c. **Ensuring** that the requirements of this directive are included in facility review and acceptance criteria for new facilities and office spaces both FAA owned and leased.

**25. RESPONSIBILITIES OF THE ASSOCIATE ADMINISTRATOR FOR CONTRACTING AND QUALITY ASSURANCE, ASU-1.** The Associate Administrator for Contracting and Quality Assurance is responsible for ensuring that the meaning and intent of the provisions of this directive pertaining to contract guard force standards and requirements are included in national contracting policy guidelines.

**26. RESPONSIBILITIES OF REGIONAL PROGRAM AND PROJECT MANAGERS.** Regional program and project managers are responsible for:

a. **Coordinating** with the appropriate SSE for security support during the initial phases of new project design and planning.

b. **Ensuring** that the SSE is included in design meetings and discussions that will determine the design and architectural characteristics of the new construction or modification.

c. **Taking positive action** to ensure that the program architects and designers include in facility planning and design those physical security standards and requirements identified by the SSE in accordance with this order.

**27. RESPONSIBILITIES OF FAA FACILITY MANAGERS.** Managers of FAA facilities are responsible for:

a. **Implementing** the appropriate PSMP policies and procedures contained in this order, contingent upon available resources and budget approval.

b. **Coordinating** with the appropriate SSE in establishing physical security planning and requirements.

c. **Taking corrective actions** in a timely manner in accordance with recommendations made by the SSE as a result of surveys, inspections, or other security evaluations of a facility.

d. **Establishing** a Facility Physical Security Management Plan (FPSMP) when recommended by the SSE.

e. **Requesting** resources and budget approval.

**28. RESPONSIBILITIES OF FAA AND CONTRACTOR EMPLOYEES.** FAA and contractor employees are responsible for:

a. **Compliance** with the requirements of this order and the PSMP.

b. **Use of good judgment and reasonable care** in safeguarding and controlling Government property issued officially to the individual or otherwise officially entrusted to his/her care.

c. **Reporting** to the immediate supervisor, manager, contracting officer representative, or SSE any security weakness or practices involving fraud, waste, or abuse of U.S. Government property.

**29.-199. RESERVED.**



## CHAPTER 2. PHYSICAL SECURITY ACCREDITATION

**200. OBJECTIVE.** Physical security accreditation is a process designed to assist facility management in applying the standards of the PSMP to the reduction of risk and vulnerability at their particular facility. It accomplishes this objective by advising the facility manager what actions, if any, he or she must take to meet the applicable physical security management and safeguarding requirements established by the PSMP. Accreditation is based on the results of the comprehensive physical security survey and accreditation evaluation.

**201. ACCREDITATION/EVALUATION.** The accreditation is conducted by the SSE to evaluate compliance with FAA orders, regulatory requirements, inspections, and surveys.

**202. ACCREDITATION/EVALUATION APPROVAL.** Accreditation certification will be accomplished as prescribed in Appendix 16 of this order. Distribution of accreditation letters shall be accomplished as follows:

**a. Regional and Facility Copies.** The original accreditation letter along with copies two and three shall be sent to the facility's respective regional office for distribution and retention. Copy two shall be retained by the region as a permanent record. Copies one and three shall be retransmitted to the evaluated facility by the region. The original letter and each copy shall be numbered as follows: "one of six," "two of six," "three of six," ... Copy numbers shall be stamped or typed on each page of every letter prior to transmission by the SSE for accountability and distribution purposes.

**b. Permanent File Copies.** The original accreditation certification letter along with copy three shall be maintained as a permanent record by the evaluated facility for review during subsequent inspections, audits, surveys, or accreditation actions. Copy four shall be maintained as a permanent record by the servicing security element. Copy five shall be transmitted to ACO-1, Attention ACO-320. Copy six shall be sent to ACP-1, Attention ACP-120.

### 203. ACCREDITATION/EVALUATION

**SCHEDULING.** Accreditation evaluations are required for all FAA facilities. Accreditation evaluations shall be scheduled by the SSE in priority of facility criticality. An accreditation evaluation may be scheduled to meet special requirements when considered necessary by the manager of the SSE. Facilities designated as critical to the NAS shall be evaluated for accreditation within 1 year after the issuance of this order. All other accreditations shall be accomplished within 2 years from the date of publication.

**204. FOLLOWUP PROCEDURES.** When an accreditation evaluation of a facility reveals vulnerabilities and/or deficiencies that require corrective action, the SSE will coordinate with the facility manager and provide advice, if required. The manager of the SSE shall ensure that recommendations for corrective action are followed up and tracked until the required actions have been completed.

### 205. CHANGES AFFECTING PHYSICAL

**SECURITY EVALUATION.** Physical security evaluation for a facility may be affected by a number of factors including changes in the environment, mission changes, increased threat levels, new construction, etc.

**a. The facility manager** is responsible for advising the SSE of any significant changes such as new construction that are planned.

**b. Comprehensive and supplemental inspections** provide an opportunity to evaluate any significant changes that might impact on the facility evaluation.

**206.-299. RESERVED.**

## CHAPTER 3. FACILITY PLANNING AND DESIGN

### SECTION 1. GENERAL

**300. OBJECTIVE.** Once a decision is made to select, construct, reconfigure a facility or office space, or move into another facility or office space, security considerations shall be an integral part of the planning, design, and construction process.

#### **301. RESPONSIBILITIES OF THE SERVICING SECURITY ELEMENT (SSE).**

a. **Site selection.** The SSE shall, whenever possible, be a participant in the site selection process.

b. **Initial facility design.** It is essential that the SSE become involved in the initial facility design, planning, and construction stages.

c. **Point of contact.** Managers of SSE shall assign a physical security specialist as the point of contact (POC) for each major facility program. To facilitate coordination, this information shall be provided to each facility program manager.

**302. RESPONSIBILITIES OF THE PROGRAM/PROJECT MANAGER.** The FAA manager having program responsibility involving design, construction and/or modification of FAA facilities and/or office spaces is responsible for:

a. **Ensuring that the appropriate SSE is informed of the program or project and included in design and planning meetings.**

b. **Ensuring that the SSE office is on the list of FAA offices provided to the architect and design engineer that will receive pertinent construction and architectural drawings and information for the program or project.**

c. **Ensuring that the SSE is an evaluator for program project design and engineering proposals.**

#### **303. NEW FACILITIES, OFFICE SPACES, AND OPERATING AREAS.**

a. **Office spaces.** Arrangements for new office spaces to be occupied by FAA elements must have provisions which enable the tenant to:

(1) Control access into the space when the assigned employees are not present.

(2) Control the removal of or the unauthorized access to property, equipment, and official records from the space.

(3) Obtain protective services when disorders or other emergency situations arise.

b. **Pre-acceptance physical security review.** Prior to the acceptance of the office space, the FAA official in charge of the element concerned shall review the adequacy of the physical security arrangements in coordination with the appropriate SSE.

(1) **National headquarters.** Plans for new facilities and office space or modifications to existing facilities or spaces by offices or services in the national headquarters shall be coordinated with ACO-300, to ensure appropriate security measures have been included in the design plans.

(2) **Regions and centers.** Plans for new facilities office space or for modifications to existing facilities or space shall be coordinated with the appropriate regional or center SSE.

#### **304. REDESIGNING EXISTING FACILITIES.**

Security planning for facilities that are to be reconfigured is as important as that for new facilities. The security costs that may be incurred through changes in the configuration of the facility (or internal movement of functions) can increase sharply if the security factors are not weighed beforehand. The redesign of a facility for the purpose of increased protection might prove to be economically sound when the cost is compared with the corresponding reduction in the theft rate and manpower that could be achieved.

**305. COMMERCIALLY LEASED SPACE.** There are a number of FAA activities occupying space in commercially owned buildings. The common arrangement is for the GSA to execute the lease on behalf of the Government. Often there will be non-FAA tenants in the building, and these typically consist of both Government and commercial occupants. From a security standpoint, this creates several problems. First, access to the FAA space, particularly after normal duty hours, cannot realistically be controlled to the same degree as in a facility where FAA is the sole occupant. Second, the FAA tenants must often rely on GSA to establish the basic protection plan for the building, and GSA must work through the building owner whenever any structural changes are to be made. Finally, there is often the problem of having to obtain security support or assistance from the SSE which may be located a considerable distance from the building. It is important that every effort be made to implement the basic security measures prior to, rather than after, occupancy. If it becomes necessary to improve security protection at

FAA-occupied, commercially leased space, the regional Real Estate Branch must be provided a written request stating the exact nature and estimated cost of the added protection. An FAA real estate contracting officer (RECO) will confer with either GSA or the lessor as appropriate to determine the negotiated method to accomplish and pay for the related work. The RECO will then advise the program office what must be included in the procurement request to fund the project.

**a. Selecting space.**

(1) Avoid, if possible, separating or scattering offices throughout the building.

(2) Attempt to locate the FAA offices on the top rather than the lower floors.

(3) If there are other FAA elements in the same building, make an effort to locate them on the same or successive floors.

**b. Controlling access into the space.** Install a locking system approved by the SSE that gives the FAA office manager effective control over who can get into the office spaces during security hours when the space is normally unattended.

(1) Provide for perimeter doors to be locked and for the locking of interior rooms if needed.

(2) Ensure effective access control and procedures for changing locks and/or cores if keys become compromised.

(3) If admittance is screened by a guard force, specify how authorized persons are to be identified.

(4) Unless cleaning and building maintenance/repair is performed during normal duty hours, determine how their presence during security hours is controlled or monitored.

(5) If elevator service is provided for the space, ensure that it does not give uncontrolled access during security hours.

**c. Controlling removal of property, equipment, and official records.**

(1) Establish a property accountability system and controls in accordance with FAA Order 4650.21, Management and Control of In-Use Personal Property.

(2) Establish property removal controls, and report all thefts to the property custodian and the SSE.

(3) Provide added protection for windows which are easily accessible from the exterior which are not under guard observation.

(4) Locate activities requiring the most protection (e.g. funds, sensitive information, etc.) in strategic locations in space with minimum vulnerability.

(5) Determine how covert exit can be prevented without infringing on safety requirements.

**d. Obtaining protective service.**

(1) Utilize available protective forces provided by GSA, the building owner, or the tenant agency.

(2) Establish liaison. When no immediate guard service is available, establish liaison with local law enforcement officials, advising them of the security hours and whom to contact in an emergency.

306.-310. RESERVED.

## SECTION 2. PLANNING AND DESIGN

**311. PERSONNEL ENTRANCES.** There are two major reasons for controlling entrances—to control access and prevent thefts. The more entrances there are the more difficult and expensive the controls become. The following shall be considered in the planning and design of facilities and office areas:

**a. Reduce the number of entrances** to the minimum consistent with the operational needs of the facility or office. To reduce the number of entrances in a facility, which is comprised of a number of separate buildings, the buildings should be grouped as close together as possible. This permits the construction of an interconnecting passageway or barrier which would allow the facility to be treated as a single building for control purposes.

**b. Locate parking in one area** on the facility site thereby creating the need for only one pedestrian gate or door for entering the facility.

**c. One entrance with aisles** to handle personnel traffic is preferred to entrances on four sides of a facility.

**d. Close one or more entrances** during slack periods when there are multiple entrances.

**312. SAFETY AND FIRE PROTECTION.** Local, state, and Federal building and safety code requirements will determine the number and type of emergency exits required for a facility or office as well as the emergency and panic hardware required for each exit. To protect against unauthorized use of these exits, the doors can be equipped

with intrusion detection alarms which will annunciate when the door is opened. Because of the close interrelationship between security, safety, and fire protection, these factors should be addressed collectively and coordinated with the appropriate FAA safety authorities in the planning of the facility or office. Particular attention should be given to the need for and location of sprinkler systems, smoke detectors, pumps, hoses, hydrants, stand pipes, etc.

**313. UTILITIES.** Utility systems that are vital to the continued operation of the facility or office shall be protected against tampering, vandalism, and sabotage. Such utilities would include, but not be limited to:

- a. Telephone and electrical closets.
- b. Power supply equipment including emergency power supply equipment.
- c. Power conditioning equipment and rooms.
- d. Main control valves and regulators.
- e. Water supply controls and distribution system.
- f. Air conditioning rooms.
- g. Transformers.
- h. Environmental control systems.

**314. ORGANIZATIONAL LAYOUT.** In the facility or office planning stages, special emphasis should be placed on the internal configuration of the facility and the proper placement of the organizational elements having security considerations. The location of a function can often serve as an effective safeguard and deterrent against unauthorized entry or theft. For example, locating the imprest fund in a segregated area that is as far removed as possible from the stairwells and elevators will reduce the vulnerability of the fund to robbery attempts.

a. **SSE responsibilities.** The SSE should ensure that once organizational elements requiring security safeguards have been identified the necessary construction features are provided for in the facility design. The SSE should also monitor the actual construction and ensure that any design change requirements have been reviewed and approved before implementation.

b. **Key organizational activities and functions.** The following activities are typical of functions that deserve special consideration in the physical layout of a facility or office:

- (1) Imprest funds, including sub-cashiers.
- (2) Automated information system (AIS) activities.
- (3) Communications centers.
- (4) Dangerous drugs and controlled substance storage areas.
- (5) Equipment storage rooms.
- (6) Firearms storage areas.
- (7) Classified information processing and storage areas.
- (8) Mailrooms.
- (9) Power and utility rooms.
- (10) Warehouse and storage areas.

**315.-322. RESERVED.**

## SECTION 3. EMERGENCY AND CONTINGENCY PLANNING

**323. GENERAL.** There are three basic types of emergency plans that must be considered by FAA facility managers; occupant emergency plans (OEP), emergency operations plans (EOP), and contingency plans.

### **324. EMERGENCY OPERATIONS PLAN.**

Emergency operations planning deals with the FAA emergency operations and procedures for coping with the effects of a national emergency or major disaster. Complete information concerning emergency operations planning requirements is contained in FAA Order 1900.1, Emergency Operations Plan.

**325. CONTINGENCY PLAN.** Contingency planning for the FAA is a requirement under provisions of section 302(e), FAA Act of 1958 (49 USC 1342(e)) and is also covered in FAA Order 1900.1.

**326. OCCUPANT EMERGENCY PLAN (OEP).** The OEP is defined by the Federal Property Management Regulation (FPMR) as "...a short term emergency response program [that] establishes procedures for safeguarding lives and property during emergencies in particular facilities." The OEP has two components, the first is the development of procedures to protect life and property, the second is the

formation of an occupant emergency organization (OEO) within each office or facility, comprised of employees designated to undertake and perform the specific tasks outlined in their OEP.

**327. RESPONSIBILITY.** The FPMR places responsibility for managing emergencies in a federally owned or leased facility upon a "Designated Official," who is "...the highest ranking official of the primary occupant agency or ... a designee selected by mutual agreement of occupant agency officials." (FPMR Part 101-20.003, Definitions). This person is responsible for developing, implementing, and maintaining an OEP as defined in FPMR Part 101-20.003(w). The designated official's responsibilities include establishing, staffing, and training an OEO with agency employees. GSA is required by the FPMR to assist in the establishment and maintenance of such plans and organizations.

**328. FAA OFFICES AND FACILITIES.** In each FAA manned office or facility under FAA control, the office or facility manager or his or her designated representative shall be appointed as the "designated official." An alternate designated official shall also be appointed. The designated official, in accordance with FPMR Part 101-20.003(g), shall be responsible for developing an office or a facility OEP, and for establishing and staffing an office or facility OEO. The FAA designated official should request the assistance of the SSE and the GSA in the formulation of the OEP and the indoctrination and training of the OEO.

**329. FAA OFFICES IN GSA-CONTROLLED FACILITIES.** In accordance with FPMR Part 101-20.103.1, the GSA will provide standard protection services for properties under its control by coordinating a comprehensive Occupant Emergency Program.

**330. FAA-LEASED SPACE.** In leased space, FAA will solicit the assistance of the lessor in the establishment and implementation of plans.

**331. INITIATING ACTION UNDER THE OEP.** The FPMR Part 101-20.103.5, provides for the following:

**a. The decision to activate the OEO shall be made by the designated official, or by the designated alternate official.** Decisions to activate shall be based upon the best available information, including an understanding of local tensions, the sensitivity of target agency(ies), and previous experience with similar situations. Advice shall be solicited when possible from the SSE, from the GSA building manager, from the appropriate Federal Protective Service official, and from Federal, state, and local law enforcement agencies.

**b. When there is immediate danger to persons or property, such as fire, explosion, or the discovery of an explosive device (not including a bomb threat), occupants**

shall be evacuated or relocated in accordance with the plan without consultation. This shall be accomplished by sounding the fire alarm system or by other appropriate means.

**c. When there is advance warning of an emergency, the designated official shall initiate appropriate action according to the plan.**

**d. After normal duty hours, the senior Federal official present shall represent the designated official or his/her alternate and shall initiate action to cope with emergencies in accordance with the plan.**

**332. TERRORIST DEMANDS, THREATS, OR ACTIONS.** The FAA OEP shall contain specific guidance on planning and action to be taken in response to demands, threats, or actions by terrorist groups.

**a. Blackmail, hostage threats, or attempts.** FAA facility and office managers shall not submit to blackmail/hostage threats by terrorist groups, and will notify higher level officials and the SSE immediately upon receiving such a threat. As it is not current U.S. Government policy to yield to such threats, FAA managers will not unilaterally pay nor plan for payment of ransom.

**b. Government-owned contractor operated (GOCO) facilities.** The FAA official(s) having supervisory responsibility for a GOCO facility will develop plans which provide an appropriate response to ransom threats or demands. The official(s) shall develop, in coordination with the SSE, appropriate alternative emergency plans if the contractor, having been fully apprised of U.S. Government policy concerning ransom payment, indicates an intent to yield to such threats rather than accept the risk.

**333. RELATIONSHIP TO THE PSMP.**

**a. Surveys and inspections are conducted as part of the PSMP.** All facilities under the PSMP shall be required to prepare an OEP, and establish and provide training for the OEO in accordance with applicable provisions of FPMR Part 101.

**b. Facility managers should coordinate the planning and development of the facility OEP with the SSE to ensure that detailed security guidance is provided in the plan.**

**c. Facility security management plan (FSMP).** A copy of the facility OEP should be an annex to the Facility Physical Security Management Plan (FPSMP) for those facilities that are required to have a FPSMP. For all other FAA facilities, the OEP should be maintained in a location where it is readily accessible.

**334. BOMB THREATS.** The OEP should include specific measures to be taken in the event the facility or office receives a bomb threat or experiences a bomb incident. Appendix 4 contains guidelines for preparing to cope with bomb threats, as well as a sample bomb threat checklist.

**a. Procedures for handling bomb threats** should include personnel awareness on the part of employees achieved through training and lectures by SSE, GSA, or explosive ordnance disposal (EOD) personnel. Training should include procedures for handling bomb threats, bomb search procedures, damage control procedures, and post incident recovery procedures.

**b. Mail room personnel and personnel who work in package delivery areas** should be trained on the distinguishing characteristics of letter and package bombs. Training of this type as well as informative literature and illustrated charts are available from the GSA and from Department of the Treasury, Bureau of Alcohol, Tobacco and Firearms, Washington, D.C. 20226. Assistance in obtaining materials of this type may be obtained through the appropriate SSE.

**c. Control measures** that are part of the facility or office PSMP can assist in lessening the chances that bomb threats or bomb incidents will successfully achieve their intended impact. Control measures should be intensified during periods of disturbance or any other indication of dissidence or dissatisfaction. Especially important in this regard are personnel identification and package, mail, and material controls.

(1) All building occupants especially security and maintenance personnel should be alert for persons who look or act suspiciously, and should report such persons to their immediate supervisor and the security guard force.

(2) Suspicious objects, items, or parcels. Personnel should be instructed to report suspicious items or parcels, which do not appear to belong in the area, to their immediate supervisor. They should be trained to report and not touch or attempt to move such items.

(3) Control access to utility closets, boiler rooms, fan rooms, telephone wire closets, switchboards, washrooms, and elevator machinery rooms. These and similar areas are vulnerable and should be kept locked to prevent unauthorized access. Keys must be readily available however, in the event a search is necessary.

**d. Handling bomb threats** correctly requires training and awareness on the part of facility personnel. Bomb threats may be received either by telephone or by written message. The actions to be taken upon receipt of a bomb threat should be clearly spelled out in the OEP. Bomb threat checklists (refer to appendix 4) should be placed at those telephones where a threat is most likely to be received, and personnel should be trained in their use.

**335. CIVIL DISTURBANCES.** Civil disturbances are group acts of violence and disorders prejudicial to public law and order and may have an effect on the physical security of an FAA facility. The facility or office OEP must contain provisions for actions to be taken to protect personnel and property in the event of civil disturbances.

**a. Coordination.** The OEP must provide for coordination with local, state, and Federal law enforcement and governmental authorities as well as with the SSE.

**b. Responsibilities.** The OEP should prescribe specific responsibilities for all actions required to protect personnel and property during a civil disturbance to include designation of priorities of protection, based on analyses of criticality and vulnerability.

**c. Practice.** The civil disturbance portion of the OEP must be continuously reviewed, and revised based on all available intelligence concerning the causes and extent of actual or potential disturbances, and on the guidance provided from local, state, and Federal governmental sources.

**336. TESTING OF OEP.** The OEP must be tested with sufficient frequency to ensure that the guidance contained in the plan is current and appropriate, and that the plan covers all pertinent areas of concern to the particular facility. It is recommended that those portions of the OEP that can be tested without disrupting operations be tested at least once during each 90-day period. To the extent that is possible, a full scale test of the OEP should be held at least once during each calendar year.

**a. Practical exercises.** Wherever possible, practical exercises under conditions of a simulated emergency or contingency situation should be conducted. Each exercise or test should have a specific objective.

**b. Review.** Portions of the plan which cannot be readily tested in a practical exercise should be carefully reviewed and updated as necessary. Information concerning procedures, locations of emergency aids, routes of emergency ingress and egress to and from the facility, other agencies which will be depended upon to assist, and similar data must be accurate and should be updated as required.

**c. Records.** The designated official is responsible for ensuring that detailed records are kept of all tests and exercises to include results and recommendations for improving the OEP. Records shall also indicate the actions taken to identify and correct weaknesses noted during each exercise. The SSE will inspect these records during each survey and inspection of the facility.

**337.-399. RESERVED.**

## CHAPTER 4. PHYSICAL SECURITY RISK ANALYSIS

**400. OBJECTIVE.** Physical security risk analyses of FAA facilities are conducted to determine the criticality, vulnerability, and threat associated with the asset to be protected. The probability of each identified threat causing a serious loss or disrupting the mission shall also be addressed along with the operational impact to the National Airspace System (NAS). Monetary assessments of asset value and replacement cost, together with an estimate of time required to replace or restore the asset, shall be coordinated with the appropriate acquisition and systems engineering offices.

**401. RELATIONSHIP TO THE PSMP.** A risk analysis shall be included as part of the final report for each facility physical security survey conducted by the SSE. The risk analysis shall be used by the SSE to assist in identifying vulnerabilities and appropriate countermeasures.

**402. CRITICALITY.** The criticality of a facility or asset is simply its importance to the FAA and the NAS. The first step in the risk analysis process is to determine, as accurately as possible, the importance or criticality of the facility, and the impact that damage or loss of the facility or disruption of the operation would have on the FAA and the NAS.

**403. REPLACEMENT.** In addition to the impact of loss or damage to the facility on the NAS, the criticality of an asset also depends on how readily the asset or the function it performs can be replaced.

**404. CONCEPT OF RISK.** Risk is the probability that an asset will suffer loss or damage from exploitation of vulnerabilities that are associated with a facility, or from actual or potential threats, or a combination of vulnerabilities and threats.

**405. PHYSICAL SECURITY THREATS.** A physical security threat exists when a natural threat, or a human threat, is identified that has the capability of causing damage to or loss of the facility. In the case of a human threat, risk analysis considers both the capability to cause damage or loss and the human intent.

**406. TERRORIST THREAT TO FAA FACILITIES.** Servicing security elements shall include in the conduct of each risk analysis an evaluation of the possibility of a terrorist threat to the facility or asset. If vulnerabilities exist that would facilitate the success of such an attack they shall be identified and quantified to the extent possible.

**407. OBTAINING THREAT INFORMATION.** In developing risk analyses the SSE shall coordinate with appropriate law enforcement and security agencies at the regional level and ACI at the national level to acquire information regarding possible threats to FAA facilities.

**408. COUNTERMEASURES.** Countermeasures are specific actions designed to eliminate or reduce a vulnerability and to control risk. A specific countermeasure may be a physical modification, a procedural change, or other measure.

**409.-499. RESERVED.**

## CHAPTER 5. FAA FACILITY SECURITY STANDARDS PERIMETER AND EXTERIOR CONTROLS

**500. OBJECTIVE.** To establish physical security standards for perimeter and exterior asset and building control.

**501. APPROACH.** Every FAA facility requires some degree of physical security to provide adequate physical security safeguards for FAA employees and to safeguard U.S. Government property and assets from loss, theft, damage, unauthorized use, criminal acts, espionage, sabotage, and

terrorism. The type and degree of physical security safeguards applicable to a specific facility will depend upon the assets to be protected, as well as the criticality of the facility and its vulnerability. Facility managers are responsible for ensuring that adequate physical security safeguards are provided for U.S. Government property and assets under their control. The SSE is responsible for ensuring that facility managers are informed of the safeguarding requirements for their facility through the survey and inspection process.

### SECTION 1. PERIMETER BARRIERS

**502. PERIMETER CONTROLS.** Perimeter protection is the first line of defense in providing physical security for a facility. Protecting the outer perimeter of a facility may be accomplished by installing fences or other physical barriers, exterior lighting, perimeter intrusion detection systems (PIDS), or by a guard force. Often a combination of two or more of these controls will be the most effective.

#### **503. PURPOSE OF PERIMETER BARRIERS.**

In addition to defining the physical limits of a facility and controlling access, a perimeter barrier also:

- a. Provides a support base for mounting a PIDS to provide an interactive barrier.
- b. Creates a physical and psychological deterrent to accidental entry.
- c. Deters unauthorized entry.
- d. Aids the guard force in controlling access.
- e. Facilitates the effective utilization of the guard force.
- f. Provides flow control capability for persons and vehicles through designated entrances.

**504. FAA STANDARD SECURITY FENCE.** Large operational FAA facilities such as Air Route Traffic Control Centers (ARTCC) will normally have requirements for an FAA standard security perimeter barrier fence. Construction of an FAA standard security perimeter fence shall be accomplished in compliance with specifications contained in Appendix 5 of this order and engineering guidance contained in FAA-E-2065. Conflicts between the guidance contained in FAA-E-2065 and this directive should be brought to the attention of the SSE or ACO-300 without delay.

**505. CLEAR ZONE.** The FAA standard security fence shall be constructed so that an unobstructed area or clear zone is maintained on both sides of the barrier. For design and engineering purposes the interior clear zone should be at least 30 feet (9.14 meters) in width. The outside clear zone should be a minimum of 20 feet (6.09 meters) or greater in width.

a. A fence that is not protected with PIDS and closed circuit television (CCTV) is likely to be very vulnerable to attack and unauthorized access if it is not under constant guard surveillance. The purpose of the clear zone is to make it more difficult for a potential intruder to conceal himself or herself from observation.

b. The clear zone should be free of any object or feature which would offer concealment (such as a physical structure or parking area) or which could facilitate unauthorized access (such as an overhanging tree limb).

**506. WHEN THE CLEAR ZONE REQUIREMENT CANNOT BE MET.** When for operational, environmental, or other reasons it is not practical to establish the required clear zone at a facility, the SSE shall coordinate with the facility manager to develop compensatory measures. The SSE will evaluate the risk and vulnerability associated with the fence and recommend appropriate countermeasures which may include increasing the height of portions of the fence; providing increased lighting in the affected area; CCTV surveillance cameras monitored from a remote location; installation of PIDS; and guard patrols.

**507. GROUNDING.** Fencing shall be grounded in accordance with requirements of FAA-STD-019.

**508. CONSTRUCTION.** See Appendix 5 for detailed requirements for construction of the FAA standard security fence.



**509. GATE ENTRANCES.** The number of perimeter gates which are designated for active use shall be kept to the absolute minimum required for operations. This means that provision shall be made for sufficient entrances to accommodate the peak flow of both pedestrian and vehicular traffic, as well as provision for adequate lighting and efficient inspection.

**510. UNATTENDED GATES.** Gates that are not manned shall be securely locked at all times. Protective lighting shall be provided to deter attempts at tampering during the hours of darkness. PIDS and CCTV protective measures shall be considered when determined to be necessary to meet safeguarding requirements.

**511. SEMI-ACTIVE GATES.** Gates which are used occasionally shall be protected in the same manner prescribed for unmanned gates during those periods when the gate is not under the direct visual observation and control of a security officer.

**512. GATE CONSTRUCTION.** See Appendix 5, section 2, for detailed specifications on the construction requirements for perimeter gate structures.

**513. PERIMETER WARNING SIGNS.** FAA warning signs identifying facilities as important to air safety and warning against trespass or attempts to damage the facility shall be affixed to all FAA standard security fences and to FAA buildings and structures in accordance with the following requirements:

a. **Fences.** FAA warning signs shall be affixed to all FAA perimeter fencing at intervals of 50 feet. In areas where the use of a second language other than English is prevalent, bilingual warning signs shall be installed.

b. **Buildings and structures.** FAA warning signs shall be affixed to the exterior of all FAA Air Traffic buildings and structures. Building and structure warning signs shall be installed on the building or structure not more than 50 feet apart. For irregular shaped and smaller buildings and structures, the signs shall be posted in such a way that they are plainly visible to anyone approaching the building or structure.

c. **Procurement.** FAA warning signs may be procured from the FAA Depot, Oklahoma City. The signs have been printed on two materials, metal and heavy paper card stock. The stock numbers are NSN 9099-00-056-9704 (metal) and NSN 9099-00-056-9703 (paper).

**514. PROTECTION IN DEPTH.** On a very large facility complex, such as the FAA Technical Center, it may be difficult to construct a perimeter fence that can be maintained under constant observation. Facilities of this type may also have multiple buildings with different safeguarding requirements. It will be necessary for the facility manager(s) to work closely with the SSE to identify the most cost effective types of perimeter safeguards. Creating "islands" of security around specific vital facilities, the posting of warning signs, the reduction or control of access roads, and the conduct of periodic patrols between the outer perimeter and the individual facility perimeters are measures which may be considered.

**515. ALTERNATIVE BARRIERS.** Perimeter barriers other than the standard FAA security chain link fence may be required under some circumstances. Utilization of alternative barrier structures for applications that would normally justify a standard security fence shall require the prior approval of ACO-300.

## SECTION 2. PROTECTIVE LIGHTING

### 516. OBJECTIVES.

The objectives of protective lighting are to:

a. **Discourage or deter attempts at entry by intruders** during hours of darkness.

b. **Increase the probability of detection of attempts at intrusion.**

c. **Permit the identification and inspection of persons and vehicles entering or departing the facility premises through designated control points.**

**517. DESIGN STANDARDS.** Refer to Appendix 6, of this order for standard design requirements and standards for protective lighting.

**518. APPLICATION.** Protective lighting should not be used as a psychological deterrent only. It should be used on a perimeter fence line only where the fence line is under continuous or periodic observation. Where protective lighting is required it shall be of the continuous type as defined in Appendix 6.

4/16/93

**519. ACTIVE ENTRANCES.** Pedestrian and vehicle entrances shall be provided with two or more lighting units installed in such a way that they provide adequate illumination for recognition of persons and examination of credentials.

**520. SEMI-ACTIVE AND INACTIVE PERIMETER ENTRANCES.** Pedestrian and vehicle entrances that are semi-active or inactive shall have the same degree of continuous lighting as the remainder of the perimeter. In addition, standby lighting (refer to Appendix 6 for definition) shall be used to provide required levels of increased illumination when the entrances become active.

**521. CRITICAL ASSETS.** Under certain circumstances, it may be desirable not to attract attention to specific critical assets on a facility by the use of continuous lighting. In these cases manually operated protective lighting shall be installed to enhance visual surveillance capabilities in the event of an emergency or suspicious activity in or near designated critical areas. Supplemental IDS protection of critical assets is also required for continuous electronic surveillance. Intrusion Detection System applications of this type shall be approved by the SSE.

**522. PARKING LOT AREAS.** Parking lots shall be provided with uniform illumination of 4 - 5 foot candles. In addition to the security hazard of providing hiding places, parking lots are vulnerable to pilferers and can pose a risk to employees from the standpoint of vulnerability to physical attack.

**523. SECURITY GUARD GATE HOUSES.** Gate houses at entrance points shall have a reduced level of interior illumination to enable the guards to see better, increase their night vision adaptability and avoid making them a target.

**524. EMERGENCY POWER.** Whenever feasible protective lighting systems at FAA facilities shall be connected to the emergency power system to ensure they remain operational during periods when commercial power is interrupted.

### SECTION 3. VEHICLE AND PARKING CONTROL

**525. SELECTION OF PARKING AREAS.** Whenever possible parking areas for vehicles owned by FAA employees shall be located inside the perimeter of the protected areas.

#### **526. PARKING AREA REQUIREMENTS.**

a. **Fence.** Parking areas should be fenced and well lighted.

b. **Area marking.** The method of parking should be clearly indicated (e.g. head-in, parallel, etc.) and strictly enforced.

**527. GUARD MONITORING.** The facility guard force shall monitor the parking lot activity by patrol at least once during each guard shift and on a spot check basis.

**528. VISITOR PARKING.** Areas designated for use by visitors shall be clearly identified and located so that they are under the surveillance of the contract guard force personnel.

### SECTION 4. PERIMETER IDS

**529. PERIMETER INTRUSION DETECTION SYSTEM (PIDS).** Personal observation remains an important means for perimeter protection. In many large FAA facilities such as ARTCC's, such observation is usually limited to that performed by periodic patrols. Usually, only a portion of the perimeter barrier is within the field of observation of the guard house at these locations. The value of an ARTCC (more than \$450,000,000) and its vital role in support of the NAS are factors which shall be considered by the SSE in evaluation of perimeter security

safeguards. The installation of a PIDS to provide a continuous surveillance capability for the perimeter of an ARTCC and similar large FAA facilities should be considered where it is determined on the basis of risk analysis to be necessary to meet safeguarding requirements.

## SECTION 5. BUILDING CONTROLS

**530. GENERAL.** After perimeter safeguards have been established, the next concern relates to the exterior building controls. For FAA facilities that do not have a perimeter security fence, the exterior of the building becomes the perimeter. In these instances, the building exterior serves as both the primary and secondary lines of security safeguards. This section and Appendix 7 establish physical security criteria and standards that are applicable to the building exterior.

**531. DOORS.** Doors represent a vulnerability if they are not properly constructed and controlled. Control of access to any facility is directly related to the ease with which unauthorized persons can enter or leave the facility. Doors become an important factor in establishing reasonable levels of control to minimize the possibility of unauthorized access to sensitive or controlled areas.

**532. NUMBER OF ENTRANCES.** The number of active doors that can be used to gain access to an FAA facility or office shall be kept to the minimum necessary to support operations. Doors which are not essential shall be locked or controlled by an approved access control system. Doors which are identified as entrances shall be located in such a way that visitors must identify themselves to a receptionist or a security officer before proceeding further.

**533. CONSTRUCTION.** Door and frame construction is important as a primary physical safeguard against unauthorized access to buildings and structures. There are many different types of doors and many factors which affect the security provided by door construction. Architectural conformity and concern for aesthetics often require that door structures be less substantial than desired. Appendix 7 summarizes basic physical security requirements for door construction.

**534. WINDOWS.** Window openings, like doors, can be inviting targets for potential intruders. They also can serve as an alternative means for removing U.S. Government property and documents from a facility. Windows, like doors, have an aesthetic value, and when considering security safeguards, these concerns must be addressed. Fire and safety concerns also must be coordinated by the SSE when considering measures that would affect window openings.

**535. SECURITY CONCERNS.** Any part of a window that is 18 feet (5 meters) or less above ground or 18 feet (5 meters) or less from a potential access point such as an adjoining building, tree, etc., shall be considered as vulnerable to access. Windows that are potential points of access shall be provided with locking devices, protective

screens, security grills, or other appropriate safeguards to ensure that they provide an effective deterrent to their use for unauthorized or illegal purposes.

**536. WINDOW CONSTRUCTION.** Appendix 7, section 2, contains specifications for safeguarding windows and frames.

**537. MISCELLANEOUS OPENINGS.** Many FAA facilities have manholes which provide entrances into the buildings for service purposes. Manholes may provide access to utility tunnels containing pipes for heat, gas, water, telephone transmission conduits and cables, and other utilities. Other openings which provide potential points of access either to the facility or to vital assets or services supporting the facility include:

- a. Ventilating grills.
- b. Utility grates.
- c. Sewers and storm drains.
- d. Building and roof openings.
- e. Skylights, transoms.
- f. Ventilating shafts and ducts.

**538. REQUIREMENT.** Any opening that provides a potential point of access to a facility or to vital portions or elements servicing the facility shall be identified. Appropriate physical security measures shall be implemented to ensure that unauthorized access to openings of this type is not possible without detection.

**539. SAFEGUARDS FOR MISCELLANEOUS OPENINGS.** Appendix 7, section 3, provides specifications for application of physical security safeguards to various types of miscellaneous openings.

**540. FIRE ESCAPES.** Exterior fire escapes usually do not provide entrance directly into a building. However, if a fire escape is not properly designed, it can provide a potential intruder with an easy access to the roof or to openings high above the ground level. Physical security safeguards must be coordinated with appropriate fire and safety officials to ensure that fire escapes do not interfere with emergency systems, procedures, or equipment. In some instances it may not be possible to reduce completely the physical security hazard posed by a fire escape or similar safety feature. In these cases, alternative security measures shall be considered. Alternative measures would include, for example, the utilization of CCTV, IDS, and guard patrols.

4/16/93

a. **Windows or other openings** leading off the fire escape should be secured if they provide potential access points for an intruder. Measures taken to secure windows will be coordinated with the appropriate fire and safety officials to ensure that they do not impede safety processes.

b. **The fire escape should not extend all the way to the ground.** If it is not possible to correct this weakness (i.e., the fire escape must reach all the way to the ground for safety reasons), the SSE shall work with the facility manager and the appropriate fire safety officials to provide alternative safeguards.

c. **Coordination with fire and safety officials** should be established with regard to any security measures directly affecting the fire and safety systems and procedures for an FAA building, office, or operating area.

**541. WALLS.** Wall structures are normally not considered possible points of entry because of their usual solid construction. Walls however cannot be disregarded because intruders have been known to break through wall brick and masonry barriers to gain access to a facility or an asset. An example of a hazard in this regard would be a common wall between two buildings, particularly if one of the buildings is of light construction or not properly secured, allowing a potential intruder to gain access.

**542. WALL SAFEGUARDS.** When a vulnerability is identified with a wall separating the FAA space from adjacent non-FAA offices or areas, the SSE, in coordination with the facility manager, shall develop countermeasures to reduce the vulnerability to an acceptable

level. In developing countermeasures, the objective should be to provide at the wall location a level of physical security that is at least commensurate with the value of the assets being protected and the element of risk involved. Countermeasures which may be considered include, but are not limited to, the following:

a. **Extending wall construction to ceiling or roof deck.** This is often possible when the vulnerability is due to a wall that does not extend from floor deck to ceiling deck providing the potential for access over the top of the wall. Physical enhancement would involve construction extending the wall to the ceiling deck or construction of an expanded metal barrier to close the intervening space between the top of the existing wall and the ceiling deck. When the primary concern is to detect unauthorized access attempts rather than to deter or provide a substantial physical barrier, lightweight construction, such as plasterboard can also be used. When lightweight materials are used, consideration shall be given to installation of an IDS in the ceiling space to detect attempts at forced entry.

b. **Reinforcing wall.** Covering the entire wall with 9-gauge expanded metal may be appropriate in some instances.

c. **Use of IDS sensors.** If the primary concern is that entry may be possible by forcible means without detection as might be the case in a storage room or similar area, the use of alarm sensors may be an effective solution. Vibration detectors placed on the wall surface provide a reliable means for sensing and reporting to an alarm monitor attempts at forcible entry through the wall. IDS applications shall be developed in coordination with the SSE and shall comply with requirements of Federal Specification W-A-450C, Interior Sensors and Components.

**543.-550. RESERVED.**

## SECTION 6. GUARD FORCE

**551. OBJECTIVE.** A well-trained and equipped security guard force provides management with an effective means for implementing and monitoring the provisions of the PSMP at major FAA facilities such as ARTCC's. The guard force is an extension of management and, when properly supervised and employed, represents a major capability for risk reduction through effective implementation of management's PSMP policies and procedures.

**552. DETERMINATION OF NEED.** Managers of FAA facilities should coordinate with the SSE to evaluate the need for contract security guard support for new facilities or for facilities that do not presently have such support. For facilities that have contract guard service, the facility manager should

coordinate with the SSE to ensure that the contract guards are being used in the most effective manner to accomplish the goals of the PSMP.

**553. CONTRACT GUARD REQUIREMENTS.** Appendix 8, Standards for Contract Guard Force, establishes the minimum FAA standards which are to be met by any provider of contract guard services to an FAA facility.

a. **SSE's are responsible for ensuring that the information contained in Appendix 8 is included in any Request for Bid or Statement of Work for contract guard services prepared at all regions and centers.**

**b. The manager of the FAA office requesting contract guard services shall ensure that the SSE review any Statement of Work or Request for Bid for security guard services prior to submission of the request to the appropriate contracting office.**

**c. The SSE will ensure during its survey and inspection coverage of a facility that the requirements of this section have been met.**

**554.-599. RESERVED.**

4/16/93

## CHAPTER 6. FAA FACILITY SECURITY STANDARDS INTERIOR AND ASSET CONTROLS

### SECTION 1. CRITICAL AREAS

**600. GENERAL.** The third line of protection for a facility is interior controls and safeguards. Some critical areas by necessity have to be controlled if the objectives of establishing reasonable safeguards for internal security are to be achieved. The extent of the interior controls within FAA facilities will be largely determined by the value and importance of the items, operations and areas to be protected, and the vulnerability of the facility to unauthorized entry both during and after normal working hours. The SSE, through surveys, inspections, and technical advice, supports the facility manager by identifying the assets to be protected and by quantifying, to the extent possible, the factors of criticality, vulnerability, and risk. The SSE shall also identify specific countermeasures to reduce vulnerabilities where appropriate. The facility manager is responsible for taking appropriate action to reduce the identified vulnerabilities.

**601. CRITERIA FOR THE DESIGNATION OF CRITICAL AREAS.** The identification of an area as critical depends upon a number of factors. Areas that are critical to a major facility, such as an ARTCC, may not be identical to those that are critical to an Automated Flight Service Station (AFSS) or to a Long Range Radar (LRR) facility. The facility manager of each facility shall coordinate with the SSE to identify those areas that are critical. An area should be designated as critical if it meets one or more of the following criteria:

**a. The area is one that is necessary for the continued operation of the facility, and one which would be difficult to duplicate or restore. Examples:**

- (1) The power conditioning system (PCS) area.
- (2) The air conditioning system control area servicing air traffic control (ATC) computer rooms.
- (3) Communications facilities such as air-ground ATC communications; radar data links; intrafacility ATC communications; emergency communications; demarcation areas; voice switched communications systems.
- (4) Water supply system.

**b. The area is one that requires controlled access by Public Law, national policy, or agency directive. Examples:**

- (1) Computer rooms. (PL 100-235, FAA Order 1600.54)
- (2) Classified information processing and storage areas. (Executive Order (E.O.) 12356, FAA Order 1600.2)
- (3) Telecommunications facilities processing classified information. (E.O. 12356, FAA Order 1600.8)
- (4) Areas processing certain types of financial and contract information and data.
- (5) Areas processing and/or storing Privacy Act information. (Privacy Act of 1974, FAA Order 1280.1)

**c. The area is one in which monies or sensitive negotiable forms are maintained. Examples:**

- (1) Government travel requests (GTR) and airline tickets (including ticket stock) in travel offices.
- (2) Purchase Order Invoice Voucher (SF-44) forms in procurement or purchasing offices.
- (3) U.S. Government Transportation Request (SF-1169)
- (4) Credit cards (e.g. AT&T, Government National Credit Card (SE-149), in the issuing offices.
- (5) Official passports in travel offices.
- (6) Funds in credit unions and imprest funds.
- (7) Identification media blank forms in the issuing office.

**d. The area requires controlled access to preclude interference or disruption of the activities within the area. For example:**

- (1) Air traffic control room floors.
- (2) Air traffic control towers.
- (3) National Airspace System Management Facility.

e. The area is used for the storage of valuable or sensitive equipment or data. Examples:

- (1) Loan pools.
- (2) Loading docks.
- (3) Warehouse storage and processing areas.
- (4) Mailrooms.
- (5) Medical offices.

**602. CONTROLLING CRITICAL AREAS.** In establishing an effective system of internal area control, the facility manager shall seek the assistance of the SSE to identify appropriate administrative and operational controls. The measures selected will be determined by the type of asset being protected and FAA requirements. Measures to be addressed include:

- a. Physical compartmentation from adjacent areas.
- b. Security awareness training and employee surveillance of the area.
- c. Use of locking devices to secure room areas.
- d. Use of vaults or strongroom construction.
- e. An effective system of personnel identification (e.g. coded badges, access lists).
- f. Fixed guard post or receptionist at entrance to area.
- g. Use of electrical/mechanical personnel access control pushbutton combination locks.
- h. Integrated electronic security management system with card access.

**603. LOCKING DEVICES.** The physical security of any property or facility relies heavily upon physical locking devices. Locks must when necessary be supplemented by other security protection devices and procedures and combined into a total security system. It is essential in establishing the use of locks in interior area control that locking hardware as well as door frames and other hardware and structural features be assessed by the SSE.

**a. FAA Standard Lock System.**

On September 9, 1989, the Administrator approved procurement of locking equipment "to satisfy the FAA's needs for additional units or replacement items," under the provisions of subsection 6.302-1(b)(4) of the Federal Acquisition Regulation (chapter 1 of title 48, CFR). The Administrator authorized the procurement of locking equipment from "only one responsible source and no other supplies or requirements will satisfy agency requirements." The determination is valid for a period of 5 years and applies to the Best Universal Lock Company, Inc.'s locking mechanisms and proprietary codes.

**b. Locking mechanisms manufactured by the Best Universal Company, Inc.,** shall be used by all FAA facilities to provide physical safeguards to ensure against malicious and willful damage to FAA equipment and other assets located in manned and unmanned facilities dispersed throughout the continental United States and overseas.

**c. The FAA Standard Lock System** must be keyed to a proprietary key way and key cutting codes designed solely for the use of FAA. All locks in the FAA system should have 7-pin removable and interchangeable cores which can be changed without the necessity of disassembling the entire core.

**d. FAA facilities and/or operations** that are using other than the FAA Standard Lock System should replace existing key-operated locks with the FAA Standard Lock System as existing locks are due for replacement, become worn, broken, or compromised.

**e. Buildings that are not under FAA control.** The requirement for installation and retrofit of locks with the FAA Standard Lock System applies to FAA elements located in buildings not under FAA control to the extent that is feasible. Opposition to installation or retrofit from non-FAA building management may require that the FAA offices continue to use the system provided by the non-FAA building owner or manager. In these instances, the SSE shall assess the risk and vulnerability and identify to the FAA facility manager appropriate countermeasures to provide the necessary level of security for the area. These countermeasures may include additional enhancements such as CCTV or intrusion detection systems (IDS) if required.

**604. ISSUANCE AND CONTROL OF LOCKS AND KEYS.** An effective lock and key issuance and control system is essential to safeguard property and control access.

**a. For effective control,** accurate records shall be maintained. Key and lock control record forms shall be the type provided by the lock manufacturer unless otherwise specified by the SSE.

**b. Physical inspections of locks and locking devices** shall be conducted at least once during each 6-month period.

**c. Inventories of keys, cores, and locking devices** for which the key control custodian is accountable shall be conducted at least once during each 6-month period.

**d. Keys, locks, cores, and associated hardware** shall be stored in an approved security container or in a room or container specifically approved for that purpose by the SSE.

**e. Appendix 9,** provides specific information concerning key and lock control requirements which are applicable to all FAA facilities.

## SECTION 2. SAFEGUARDING GOVERNMENT FUNDS

### 605. PROTECTION OF GOVERNMENT FUNDS.

The physical security standards in this section apply to all Government funds which include, without being limited to, revenues and funds of the United States. Checks, bonds, etc., should also be considered as falling under this definition. A fund activity is interpreted as any FAA activity or function approved by the head of the FAA facility to handle Government funds; such as, imprest funds, disbursing offices, or collection offices. The requirements of this section do not generally apply to funds controlled by private associations which are physically located within FAA space, such as credit unions, employee recreation associations, and concessionaires. The SSE and the facility manager should encourage such activities to adopt the same or equivalent measures in order to decrease the overall vulnerability and the possibility of robbery or loss of funds. This section addresses general physical security standards which must be met to safeguard imprest funds and should be used in conjunction with the current version of FAA Order 2770.4, Imprest Fund, to determine security requirements and administrative safeguards that are required. Areas in which monies or negotiable/sensitive forms such as GTR's, airline tickets, imprest funds, purchase orders, Form (SF44), or credit cards shall be designated "Restricted Areas."

**606. SSE RESPONSIBILITIES.** The SSE is responsible for:

a. Coordinating with the imprest fund custodian to ensure that adequate protection procedures are developed and implemented.

b. Ensuring that surveys and inspections of the facility include inspections of the imprest fund security controls to verify that the procedures in this order and in FAA Order 2770.4 are being followed and that physical security controls are functioning properly (e.g., CCTV, "panic/duress" alarms, hold-up cameras, and security containers).

c. Changing or instructing authorized persons in how to change the combination(s) to the container(s) used to store funds.

d. Following up, as appropriate, on all reports received regarding the loss, shortage, or theft of funds.

**607. SAFEGUARDING CONCERNS.** The following factors should be considered by the fund custodian and the SSE:

a. The location and type of building in which the fund is situated (e.g., commercially owned building versus a Government owned or leased building).

b. The specific location of the fund (e.g., proximity to elevators and stairwells, and to exterior building exits) and whether or not it is located in an area that is physically segregated from surrounding areas as opposed to an open work space.

c. Administrative safeguards. Refer to FAA Order 2770.4.

d. Physical security safeguarding requirements. Refer to FAA Order 2770.4 and Appendix 10.

### 608. FUND STORAGE ROOMS.

For funds averaging more than \$15,000 on hand, the fund container shall be located in a storage room as an additional security safeguard. The basic design features that shall be included in the construction specifications for a fund storage room are contained in Appendix 10.

## SECTION 3. SAFEGUARDING GOVERNMENT PROPERTY

### 609. SMALL ARMS AND AMMUNITION STORAGE AND PROTECTION.

Small arms and ammunition shall only be stored and controlled in accordance with the standards and procedures contained in Appendix 11 of this order. In no case will ammunition and weapons be stored in the same container.

### 610. PROTECTION OF GOVERNMENT PROPERTY.

The protection of property, including the prevention of theft, waste, and abuse of Government supplies and equipment, is a mandatory responsibility for managers under the provisions of the Federal Managers' Financial Integrity Act (FMFIA), Public Law 97-255, passed in 1982.

a. Theft factors. Actual losses due to theft depend on a number of factors, including:



(1) The type, amount, and accessibility of the equipment and supplies and their location within the facility.

(2) The number of persons employed at the facility and the shifts worked, including overtime.

(3) The relative crime rate in the surrounding communities.

(4) The effectiveness of the property management program in terms of conducting physical inventories of accountable property and promptly reporting unexplained shortages or known thefts to the SSE, especially for that property identified as "sensitive" or "high risk."

(5) The adequacy of the external and internal physical security controls, plus, for example, the use made of specialized devices for securing in-place office equipment.

(6) The degree to which employees understand and discharge their responsibilities for the safeguarding of U.S. Government property.

**611. THEFT TARGETS.** FAA property records contain in excess of \$2.1 billion of in-use personal property, and this figure is growing each year as the NAS continues to expand. In each type of FAA facility there are areas where pilferable equipment and supplies are likely to be found. The common denominator in these and similar storage areas is that they usually contain items which lend themselves to concealment, which are of relatively high value, and for which markets are readily available. The SSE will include theft targets in all inspections and surveys and will work with the facility manager to develop appropriate countermeasures to reduce identified vulnerabilities.

## **612. SHIPPING AND RECEIVING OPERATIONS.**

Shipping and receiving operations are extremely vulnerable to systematic theft. For instance, it is here that facility employees and truck drivers have direct contact and a readily available means of conveyance which can offer a tempting opportunity for a potential pilferer. From a physical security perspective, the following apply:

a. Shipping and receiving area doors shall be kept closed when not in use.

b. Deliveries, especially those containing high-value items, shall not be left unattended for an extended period of time. Such items shall not be left unattended or improperly secured overnight or over weekends.

c. Construction of a secure holding area is one means of protecting undelivered high-value items.

**613. LOAN POOLS.** Loan pools are an inviting target because of the wide range of items that usually appear in the inventory (e.g., office equipment, recorders, video and motion picture equipment, cameras). In protecting loan pools the following requirements apply:

a. In addition to separating and securing the loan pool, administrative controls must be strictly observed. Maintaining current inventory records, establishing a limited charge-out period, and following up on overdue items, as well as limiting access to the loan pool, are all important.

b. Expendable items such as film and tapes, which are not subject to strict accountability, should nevertheless be protected in such a manner that they are not subject to unauthorized access and pilferage.

**614. GENERAL AND SPECIALIZED STORAGE AREAS.** Supplies and equipments that are stored in permanent or temporary areas or warehouses are vulnerable to theft if adequate precautionary measures are not taken. Access to storage areas containing building materials, automotive and oil supplies, tools, etc., shall be tightly controlled because of the personal use which can be made of such items. The following requirements apply:

a. Items which are not ordinarily accounted for in the property management and control system shall be afforded physical protection from unauthorized access.

b. Chargeout procedures shall be established that will help to deter employees from drawing such materials for other than official purposes.

c. In large warehouses, high-risk and high-value items shall be stored separately from the general storage area in special security enclosures of wire or chain link secured by approved combination padlocks.

**615. FOR REMOTE STORAGE AREAS.** Areas that are remote from the facility pose special problems. The SSE shall work closely with the facility manager to evaluate the most effective measures to protect such locations. The use of IDS or other special security safeguards which can be monitored from a remote location should be considered.

**616. OTHER FAA STORAGE AREAS.** Navigation aids, air traffic control towers, hangars, laboratories, research and development areas, training facilities, unmanned facilities and similar locations are vulnerable to tampering, pilferage, and interference with the operational mission. The facility manager is responsible for coordinating with the SSE to establish suitable property control and physical security safeguards for these types of areas.

## SECTION 4. THEFT PREVENTION

**617. THEFT PREVENTION MEASURES.** The specific physical security measures that apply to reducing the vulnerability to pilferage and theft should be developed by the facility manager in coordination with the SSE. The SSE will advise the facility manager on countermeasures based on an assessment of the risk and vulnerability associated with specific areas and operations. Countermeasures considered by the SSE will include, but not be limited to, the following:

- a. Establishing appropriate physical security safeguards with regard to perimeter fencing, lighting, parking area control, vehicle and pedestrian control, and railway control.
- b. Establishing an effective property removal system in accordance with the provisions of this order.
- c. Investigating all thefts and losses quickly and thoroughly.
- d. Maintaining an effective key control system.
- e. Maintaining adequate security guard force patrols to check buildings, grounds, perimeter, and locations which might be used for concealing stolen property.
- f. Installing mechanical or electrical intrusion detection (IDS) devices where practicable and where a response capability is provided to respond to an alarm condition.
- g. Storing bulk quantities of high-risk items in enclosed storage areas approved for that purpose by the SSE.
- h. Marking all tools and equipment by some mark or code so that U.S. Government property can be distinguished from non-Government property.
- i. Requiring charge out procedures for all tools and equipment.
- j. Ensuring that adequate inventory and control measures are established for all material, supplies, and equipment in accordance with requirements of FAA Order 4650.21, Management and Control of In-Use Personal Property.

**618. PROPERTY MANAGEMENT SYSTEM.** There is a direct correlation between the efficiency of the property management system in effect at an FAA facility and the theft prevention program. Each is an indispensable element of the other. The Federal Managers' Financial Integrity Act (FMFIA), Public Law 97-255, requires Federal agencies to ensure that their internal accounting and administrative controls conform to the standards prescribed by the Comptroller General, and that they provide reasonable assurances that (among other requirements) funds, property,

and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation. The Federal Property and Administrative Services Act of 1949 and associated implementing orders from Office of the Secretary of Transportation (OST) and FAA require accountability for all Government-owned property including personal property. Federal Government property, with the exception of records and real property, includes all property that is tangible, movable, and not permanently affixed to other items. Personal property includes all facilities and equipment comprising the NAS, as well as supporting personal property including automatic data processing (ADP) equipment and test equipment. A complete listing of such equipment is contained in Appendix 16 of Order 4650.21. The following considerations apply:

- a. There should be a close working relationship between the SSE and the property management office. The SSE will include review of property accountability and loss control procedures during the conduct of each inspection and survey.
- b. The most common deficiency is failure to report (usually inadvertent) on the part of the property custodian and/or the FAA facility's accountable property office promptly to the SSE any actual or suspected thefts of "in-use personal property" that come to his or her attention either as the result of inventories or by other means.
- c. It is not uncommon to find that lost or stolen property has been surveyed and "written off" by the accounting office. To prevent this from occurring, the property management procedures should make clear to the property custodians the importance of reporting any instances of loss, stolen, or missing property to the SSE, as well as reporting through property management channels.
- d. The FAA facility property management office should double-check to ensure that such reports are being submitted.

### 619. ACCOUNTABLE EQUIPMENT CATEGORIES.

During the conduct of surveys and inspections, the SSE will include a review of the adequacy of the accountability and control procedures in effect for all accountable equipment and property to include the following:

- a. Accountable items regardless of price.  
Firearms and ammunition

**b. Accountable items if above \$100.**

Adding machines/calculators  
 AIS equipment  
 Airway Facilities test equipment (portable or rack mounted)  
 Audio visual equipment  
 Binoculars  
 Laboratory and medical equipment  
 Maintenance, Repair Shop equipment, and hand tools  
 Office machines (including facsimile machines)  
 Photographic equipment  
 Portable communication or telecommunication equipment  
 Recording equipment  
 Telephones, portable or cellular  
 Typewriters

**c. Accountable items if above \$500.**

Appliances  
 Athletic equipment  
 Avionics equipment  
 Commissary equipment  
 Emergency readiness equipment  
 Fire, rescue, and safety equipment  
 Food serving and preparation equipment  
 Furniture  
 Landscaping/lawn equipment  
 Metal-working machinery  
 Ship and marine equipment  
 Tractors  
 Training equipment  
 Vehicles, special purpose

**d. All items over \$1,000 are accountable.**

**e. A common assumption is that unaccounted for property is merely misplaced or borrowed and not stolen. This assumption is misleading and should be avoided.**

**620. REMOVAL OF PROPERTY FROM FAA FACILITIES.**

An essential part of the responsibility on the part of FAA managers to prevent the waste, loss, and abuse of U.S. Government property is the establishment of a system which provides for accountability and control for items of U.S. Government property that are removed from FAA facilities for official use. It is the responsibility of each FAA facility office manager to ensure that some type of positive control and accountability system is used. The facility manager shall coordinate with the SSE to develop property removal and accountability procedures that will meet these objectives.

**621. IN BUILDINGS WHERE FAA IS THE SOLE OR PRIMARY TENANT**

and entry to and exit from the building is subject to guard coverage, the property removal procedures in this order shall apply. In buildings where FAA is not the primary tenant but where entry to and exit from the building is subject to guard coverage, the FAA office or element manager shall consult with the primary tenant and/or GSA to establish controls for removal of U.S. Government-owned or leased equipment based upon the guidance in this order, if appropriate, or upon a property pass system.

**622. IN BUILDINGS WHERE ENTRY AND EXIT ARE NOT SUBJECT TO GUARD SUPERVISION,**

the FAA facility or office manager should coordinate with the SSE to develop local procedures which will ensure that U.S. Government-owned or leased equipment is removed only with the knowledge and consent of the appropriate property custodian.

**623. PROPERTY REMOVAL REQUIREMENTS.**

These procedures are written for systems that use the security officer or guard as the key individual to check property removal forms and to verify identity. If the FAA manager responsible for the facility wishes to approve all property removals either personally or through his or her designated representative, this is acceptable, provided it is coordinated with the security guard force and that the control standards of this section apply.

**a. An individual who removes U.S.**

Government-owned or leased property, equipment owned by contractors, subcontractors, vendors, or suppliers, and equipment personally owned by FAA personnel or visitors shall present to the security guard a completed Property Removal Record, DOT F 1660.2. The form may be completed at the security guard office where a supply should be maintained for that purpose. An example of Form DOT F 1660.2 is contained in Appendix 3. This form may be requisitioned from the Distribution Branch, Department of Transportation, DOT M-494, Washington D.C. 20590.

b. The security guard shall check the completed form to ensure that the property has been described correctly and that other required data has been entered. The guard will check the identity of the individual.

c. If the individual is an FAA employee or on duty with the FAA in an official capacity and his/her identity is verified by the appropriate DOT/FAA identification card, the security guard will permit the property to be removed.

d. If the individual is an employee or representative of a contractor, vendor, or supplier and is removing equipment which has been used for demonstration or requires maintenance, etc., or if the individual is an official visitor removing equipment pursuant to a visit, the security guard shall call the FAA office listed on the DOT Form 1660.2 as having knowledge of the transaction and obtain verification. Alternatively, the FAA office having knowledge may have an FAA employee accompany the individual to the security guard station to verify the transaction. In this event, the FAA employee will identify himself/herself using his/her FAA identification card.

**624. WHEN VERIFICATION OF AUTHORITY TO REMOVE PROPERTY FROM AN FAA FACILITY CANNOT BE OBTAINED,** the security guard shall not permit the individual(s) to remove the property without the express consent of the Property Management Officer, the property custodian, or the SSE.

a. The security guard shall forward the completed DOT Form 1660.2 to the appropriate security office which, in turn, will forward the original to the Property Management Officer or the property custodian. The Property Management Officer shall contact the office of primary interest to confirm that the property has been removed for authorized purposes and, if the property is U.S. Government owned, that controls are in effect to ensure that the material is returned.

b. If the Property Management Officer/custodian cannot obtain verification for the removal, the SSE shall be notified and a theft report, if appropriate, shall be submitted through channels using GSA Form 182, Report of Loss or Theft, or equivalent region/center form. GSA Form 182 may be obtained from the General Services Administration. Other forms that have been approved by the SSE and provide the same information as the Form 182 may be used.

**625. PHYSICAL PROTECTION OF OFFICE EQUIPMENT.** Where conditions of vulnerability and risk warrant such action, office equipment, particularly items valued at \$500 or more such as typewriters, desk calculators, dictating equipment, personal computers, etc., shall, to the extent possible, be secured in place by a locking device.

a. In determining the kind and number of locking devices required for specific facility needs, the facility manager should coordinate closely with the SSE.

b. The SSE will be responsible for advising the facility manager on specific locking devices and applications, as well as on alternative security measures to accomplish the safeguarding objective where appropriate.

c. Items of lesser value which do not lend themselves to this approach, such as pocket calculators, cameras, tape recorders, and slide projectors, shall be protected at all times when not in actual use, by storing them in locked containers or rooms to which only authorized personnel have access.

**626.-631. RESERVED.**

## SECTION 5. ASSET CONTROLS

**632. DESTRUCTION EQUIPMENT.** Order 1600.2 provides that classified material may be destroyed by burning, pulping, pulverizing, shredding, or chemical processing, provided the destruction is complete and reconstruction is not possible. Under most circumstances FAA facilities will use shredders and pulverizers to accomplish the destruction of classified material. Equipment that meets the standard for destruction of classified material may also be used for the destruction of sensitive unclassified material and Privacy Act material.

a. **Shredders.** When using shredding machines, special attention must be given to ensure that the machine is of a type and model approved for the destruction of classified material by the GSA or, in the case of COMSEC material, by

the National Security Agency (NSA). Before purchasing destruction equipment or devices, facility managers shall coordinate with the SSE to ensure that the equipment selected will be adequate. The following criteria apply:

(1) **Classified information.** A shredder used to destroy classified material must meet performance requirements established by GSA or NSA and must produce a shred no larger than 3/64 of an inch in width and no more than 1/2 inch in length. Reference FAA Order 1600.2.

(2) **Sensitive unclassified information** may be shredded on any equipment approved for classified. As a minimum, shredders used for the destruction of sensitive

unclassified information shall be either strip or cross-cut and shall reduce the material to shreds no greater than 1/32 inch in width.

(3) **Privacy Act material.** Destruction of material protected under the provisions of the Privacy Act of 1974 shall be accomplished in accordance with provisions of FAA Order 1280.1.

b. **Disintegrators/Pulverizers.** The disintegrator requires a security screen with an aperture size no larger than 3/32 of an inch. Many of the disintegrator units currently in use in FAA facilities have been in service for some years. The facility manager shall ensure that the aperture size for disintegrator and pulverizer screens does not become larger due to wear on machines used for classified destruction.

c. **The SSE shall check shredders and disintegrators** to ensure that they are functioning properly as part of the survey and inspection of each facility.

**633. STORAGE EQUIPMENT.** The FAA utilizes a variety of different types of containers to meet the storage requirements for classified national security information established in FAA Order 1600.2. Appendix 12, section 1, contains detailed information on the various types of storage containers that may be considered when protecting assets including classified and sensitive unclassified material and Privacy Act information as well as sensitive forms and high risk items.

**634. VAULTS AND STRONGROOMS.** Appendix 12, section 2, contains detailed guidance on requirements and specifications for the construction of new vaults or strongrooms, or for the evaluation of existing structures. The manager of the facility or program identifying a need for a vault or strongroom should coordinate with the SSE to ensure that the standards and guidelines in Appendix 12, section 2, are applied.

**635.-699. RESERVED.**

## CHAPTER 7. FACILITY PHYSICAL SECURITY MANAGEMENT PLAN (FPSMP)

**700. OBJECTIVE.** The Facility Physical Security Management Plan (FPSMP) is a structured physical security planning process which has the objective of developing a detailed written plan to achieve adequate physical security protection and implementing measures for safeguarding against fraud, waste, and abuse in the most cost effective manner.

### 701. RESPONSIBILITIES.

a. The Facility Manager is responsible for development and implementation of the FPSMP. In facilities such as ARTCC's where there are both an air traffic and an airway facilities manager, the responsibility for development of the FPSMP shall be a joint responsibility.

b. The SSE is responsible for advising the facility manager of the need to develop an FPSMP for that specific facility.

**702. APPLICABILITY.** Because of the number and variety of FAA facilities, it is not practical to have each develop a FPSMP. In most instances, smaller operational facilities will have relatively simple security programs and systems. In larger facilities, however, such as ARTCC's, the requirement for a FPSMP is mandatory. Appendix 13 provides a listing of FAA facilities, in addition to ARTCC's because of their size, the criticality of their mission, or both, that shall be considered candidates for development of a FPSMP. In each instance, the final responsibility to develop an FPSMP will be achieved through coordination between the SSE and the appropriate facility manager or managers.

**703. PLANNING CONSIDERATIONS.** In determining the type and extent of physical security planning required at a facility or office, the following pertinent factors shall be considered by the SSE and the facility manager:

a. Mission of the facility and its criticality to the operation and support of the NAS.

b. Identification and analysis of the assets to be protected. This includes:

(1) Identification of the Government resources that are addressed under the Federal Manager's Financial Integrity Act, Public Law 97-255, and for which management is required to establish and maintain adequate controls. These resources include funds, property, and other assets that must be safeguarded against fraud, waste, and abuse. It also includes identification of those physical security concerns that are addressed in Order DOT 1600.26A, Department of Transportation Physical Security Program, dated July 25, 1990.

(2) Fixed plant cost of facility and safeguards in place to protect plant and assets against sabotage, theft, tampering, terrorist, and other criminal acts.

(3) Asset safeguards that are mandated by public law and by executive orders and National Security Decision Directives (NSDD). Included in these areas would be the Computer Security Act of 1987, Executive Order 12356, and NSDD's 97, 145, and 298.

(4) Risk analysis evaluation by the SSE with regard to the criticality and vulnerability of information, equipment, and material to compromise, damage, or theft.

(5) Operation, maintenance, and other requirements which should be included in the FPSMP.

(6) Environment, political, economic, legal, terrain, weather, and climate.

(7) Costs of material and equipment to be installed and availability of funds to provide at least minimum acceptable safeguards for all critical areas and activities.

(8) Personnel and equipment costs, and the best method of providing adequate cost-effective protection.

**704. DEVELOPING THE FPSMP.** The coordination between the SSE and the FAA facility manager concerning the FPSMP normally will take place at the time of the accreditation evaluation of the facility. A determination as to the need for the FPSMP will be included in each accreditation evaluation performed by the SSE. If determined through the coordination process that a FPSMP is required, the facility manager shall develop the plan with the advice and assistance of the SSE. The following guidelines apply:

a. The FPSMP is a physical security plan and it must be tailored to the physical security needs of each facility.

b. A basic element of the plan is a security force capable of representing management's interests in implementation of the PSMP and of ensuring enforcement of established security measures and procedures.

c. Established physical security measures and systems such as barriers, protective lighting, communications, CCTV, electronic access control systems, and other measures as appropriate will be incorporated into the plan to increase the effectiveness of the security force. The selection and utilization of security measures is the responsibility of facility security planners, the SSE, and facility managers working in close coordination.

d. The FPSMP shall contain specific guidance on:

(1) Planning and action to be taken in response to demands, threats, or actions by terrorist groups as specified in this order and the facility contingency/emergency plan.

(2) Procedures for liaison between the facility security forces and other support agencies and services to include the GSA, Federal Protective Service, fire departments, emergency medical response units, explosive ordinance disposal (EOD) teams, and local, state, and Federal law enforcement authorities.

(3) The plan should clearly identify the jurisdictional authority of the FAA facility security force (exclusive, concurrent, or proprietary).

**e. Standards of security.** Security standards established by this order, as well as standards included in the orders and directives listed in Appendix 2, shall be used as guides in planning a physical security program.

#### **705. INDICATORS.**

Indicators that might reflect deficiencies affecting a facility or office include:

**a. Evidence** that any part of the facility or office is being used for other than lawful or authorized purposes.

**b. Perimeter security** is found to be less than adequate.

**c. Fences, additional barriers, and/or protective lighting** are found to be in need of augmentation, expansion, and improvement.

**d. Personnel access controls** are found to be weak.

**e. Secure communications policies and procedures** and/or other physical security procedures are not being followed or are too awkward or slow.

**706. PLANNING GOALS.** The FPSMP shall provide physical security standards based on FAA policies and procedures for the following:

**a. Indoctrination** of personnel in the use of internal control procedures and the need for vigilance to prevent fraud, waste, and abuse of U.S. Government property.

**b. Procedures** for receiving supplies, stock control, and shipping.

**c. Safeguarding procedures** for funds to include receiving, holding, or banking money and negotiable instruments.

**d. Storing and accounting** for dangerous drugs and prescription medications. (If applicable.)

**e. Effectiveness** of security guard force and the supporting orders and procedures.

**f. Security communications systems.**

**g. Criteria** for installation of IDS and CCTV systems.

**h. Criteria** for installation of electronic access control systems (integrated security systems).

**707. FPSMP FORMAT.** A sample format for a FPSMP is included as Appendix 14 to this order.

**708.-799. RESERVED.**

## CHAPTER 8. SURVEYS AND INSPECTIONS

**800. PURPOSE.** This chapter provides the guidance required for planning, coordinating, and implementing surveys and inspections. Physical security surveys and inspections of programs in effect at FAA facilities shall be conducted in accordance with requirements specified in this directive.

**801. ESTABLISHING PRIORITIES.** Critical facilities will be assigned priorities based on criteria established by this directive and FAA Order 1650.7. Once facility priorities have been established for each region and center, the appropriate SSE shall take action to plan, schedule, and conduct physical security surveys, inspections, and/or follow-up inspections as appropriate.

**802. PROGRAM MANAGEMENT.** The Manager, Investigations and Security Division, ACO-300, is responsible for ensuring that the procedures and standards for the conduct of surveys and inspections are carried out at the regional level. ACO-300 is responsible for overall staff supervision and oversight of the security survey and inspection operations agencywide.

**803. SERVICING SECURITY ELEMENT (SSE).** Managers of Civil Aviation Security Divisions and staffs in regions and centers are the servicing security element (SSE) responsible for program management, planning, and operations within their respective areas of jurisdiction. The SSE's are responsible for ensuring that physical security program surveys and inspections are planned, scheduled, and conducted in accordance with this and other applicable directives.

### SECTION 1. SURVEYS

**804. DESCRIPTION.** The physical security survey is planned and conducted by the SSE and consists of an exacting on-site examination of the physical security program at a facility. It includes evaluation of risk and vulnerability. The results of physical security surveys are reported in writing and are used by the SSE and the facility manager to evaluate the overall physical security program effectiveness. The survey results also identify vulnerabilities that may exist and specify required corrective actions which must be taken to reduce the vulnerabilities.

**805. INITIAL SURVEYS.** The physical security survey of a facility provides information that supports the development of the Facility Physical Security Management Plan (FPSMP). The survey assists the facility manager in making determinations as to what security management controls are needed, how they will be implemented, by whom, and when. Initial surveys are required for all FAA facilities in accordance with procedures and priorities established by this order and FAA Order 1650.7.

**806. EVALUATION SURVEYS.** A survey evaluation of the entire physical security program at a facility will serve as the basis for granting or denying accreditation for the facility. Surveys are required for all FAA facilities.

**807. SUPPLEMENTAL SURVEYS.** Supplemental surveys are conducted when changes occur in the facility organization, mission, or physical features of the facility that alter or potentially affect the overall facility physical security evaluation or otherwise have a major impact on the physical security program.

**808. SPECIAL SURVEYS.** Special surveys are conducted to evaluate the impact on the PSMP when significant changes occur in specific security programs at a facility.

### SECTION 2. CONDUCT OF SECURITY SURVEYS

**809. PROCEDURES.** Appendix 15 provides guidance for the conduct of FAA security surveys. The procedures regulating the survey process, together with this chapter, establish the techniques and principles necessary to meet survey and inspection operational goals and objectives.

**810. PROGRAM EVALUATION.** Programs evaluated during a security survey include, but are not limited to, major programs such as personnel security, security education, information security (INFOSEC), communications security (COMSEC), automated information systems security (AISS), operations security (OPSEC), and physical security.



**811. SURVEY COORDINATOR.** To ensure that the planning and conduct of a security survey is carried out in the most efficient manner, the SSE manager will designate a security specialist to be the coordinator for the survey team.

**812. INITIAL PLANNING.** The extent of preparation for a survey will be governed by the size and type of facility to be visited. For large operational facilities, the coordinator should hold team meetings at key stages of the survey process. Usually the meetings are called at critical transition points, when adequate coordination of team activities is necessary, to ensure a successful survey.

**813. CONTENTS.** Surveys of FAA facilities involve many areas of concern and items to be checked and evaluated. The survey team leader or coordinator must carefully select

the area(s) which is considered critical and allocate his/her personnel and time accordingly.

**814. SURVEY TEAM MEMBERS.** Team members may be selected entirely from the staff of the SSE, or they may be selected in coordination with CASD's from other SSE's. Survey and assessment operations conducted by ACO-300, as part of its overall monitoring and oversight responsibility, will normally include representation from field security elements.

**815. SURVEY REPORTS.** The appropriate SSE will maintain copies of all initial and accreditation surveys along with current survey reports for all of the facilities within its jurisdiction. It may retain these reports in paper copy or database format and will provide copies to ACO-300 upon request.

### SECTION 3. INSPECTIONS

**816. DESCRIPTION.** Physical security inspections are also an integral part of the PSMP. Once a security survey has been conducted, inspections are scheduled on a regular basis to monitor compliance with the actions required by the security survey. The inspection also is a means for monitoring compliance with overall requirements of the physical security program. There are three basic types of FAA inspections: comprehensive, supplemental, and special.

**817. COMPREHENSIVE INSPECTIONS.** A comprehensive inspection is a review of the status of the major security program areas for a facility. It is designed also to monitor overall facility compliance with recommendations made during previous surveys or inspections. Comprehensive inspections also serve to evaluate the significance of any changes in the facility that would affect the PSMP security plan or require additional security measures.

**818. SUPPLEMENTAL INSPECTIONS.** Supplemental inspections are more narrow in scope than comprehensive inspections and are usually conducted as follow ups to monitor progress on recommendations made as a result of previous surveys or inspections.

**819. SPECIAL INSPECTIONS.** Special inspections are conducted whenever it is necessary to address security problems at specific facilities.

### SECTION 4. CONDUCT OF INSPECTIONS

**820. PREPARATION.** The special agent shall review the results of past inspections and surveys of the facility as part of his or her preparation. Reviews consist of the facility's security history, its organizational structure, the mission the facility is charged with, and data that reflect on the criticality, vulnerability, and threat profiles for the facility.

**821. ENTRANCE BRIEFING.** The facility manager will be briefed by the special agent before the initiation of an inspection. The information provided will indicate the extent of the inspection and will include a request for a point of contact while the inspection is in progress.

**822. EXIT BRIEFING.** Prior to departure from the facility, the special agent shall arrange to provide an exit briefing for the facility manager. The briefing will cover all major areas of concern that were developed during the course of the inspection, and will provide an opportunity for the specialist(s) to work with the facility manager to develop appropriate countermeasures when required.

**823. FACILITY INSPECTION REPORTING SUBSYSTEM (FIRS).** Inspections are carried out using the data collection format defined in the FIRS Checklist. This format establishes the minimum coverage requirements. It may be expanded where necessary, but the FIRS Checklist will be utilized for all inspections.

## SECTION 5. SURVEY/INSPECTION REPORTING

**824. GENERAL.** The physical security survey or inspection report subsequent to review and approval by the manager of the SSE shall be submitted through appropriate organizational channels to the facility manager of the inspected facility. The report shall include all applicable findings and requirements for corrective action.

**825. FOLLOWUP REPORTS.** When an inspection/survey results in requirements for corrective action, the manager of the SSE will ensure that follow-up action is taken. Whenever possible the Special Agent who conducted the original survey/inspection shall take this action. The purpose of the follow-up is to determine that the corrective action the facility has taken meets the related standard. The Special Agent will ensure that the results of the follow-up inspection are entered into the FIRS/PC database for the facility.

**826.-899. RESERVED.**

## APPENDIX 1. GLOSSARY OF TERMS

**Access.** The ability and opportunity to obtain knowledge.

**Access Control.** A method of providing security by restricting the movement of persons into or within a protected area.

**Accreditation—Physical Security.** The process whereby the servicing security element makes a determination as to whether or not an FAA facility meets the security standards established by this order.

**Administrative Contracting Officer (ACO).** A contracting officer who is administering contracts.

**Administratively Controlled Information.** Privileged but unclassified material bearing designator to prevent disclosure to unauthorized persons.

**Approved Built-in Combination Lock.** A combination lock, equipped with a top reading dial, that conforms to Underwriters Laboratories, Inc., Standard Number, UL 768, Group 1R.

**Approved Key-Operated Padlock.** A padlock which meets the requirements of MIL-SPEC-P43607 (shrouded shackle), National Stock Number 5340-00-799-8248, or MIL-SPEC-P-43951 (regular shackle), National Stock Number 5340-00-799-8016.

**Approved Security Container.** A security file container, originally procured from a Federal Supply Schedule supplier that conforms to federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers will be labeled "General Services Administration Approved Security Container" on the outside of the top drawer. Acceptable tests of these containers can be performed only by a testing facility specifically approved by the General Services Administration (GSA).

**Authorized Person.** A person who has a need-to-know for classified information in the performance of official duties and who has been granted a personnel clearance at the required level.

**Bomb.** An explosive device capable of producing damage to material and injury or death to personnel when detonated or ignited.

**Breach.** The successful defeat of security controls that could result in the penetration of a facility or system.

**Casual Pilferer.** One who steals primarily because he or she is unable to resist the temptation of an unexpected opportunity and has little fear of detection.

**Classified Information.** Official information regarding national security designated Top Secret, Secret, or Confidential in accordance with Executive Order 12356.

**Closed Area.** A protected area established to safeguard classified information.

**Contingency Plan.** A systematic, written plan assigning responsibilities and describing actions to be taken to reduce the impact of losses, and events with the potential for large loss.

**Controlled Area.** A general term, which for the purposes of this Order consists of both "Closed Areas" and "Restricted Areas."

**Contracting Activity.** The government activity that awards a contract.

**Contracting Officer (CO).** A government official who, in accordance with departmental or agency procedures, currently is designated as a contracting officer with the authority to enter into and administer contracts, and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his/her authority.

**Countermeasures.** A physical device, person, procedure, or combination of one or more of these intended to reduce or eliminate one or more identified vulnerabilities.

**Compromise.** The exposure of information or activities to persons not authorized access.

**Crime Prevention.** The anticipation, recognition, and appraisal of a crime risk, and initiation of some action to remove or reduce it; applies to before-the-fact efforts to reduce criminal opportunity, protect potential human victims, and prevent property loss.

**Critical Area.** That portion of a facility which is essential to continuity of operations. The partial or complete loss of which would have an immediate and/or serious effect on the capability of the facility to provide service or support to the National Air Space (NAS) operations.

**Custodian.** An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

**Disaffected Person.** A person who is alienated or estranged from those in authority.

**Duress Code.** A signal electronic or other type that is intended to indicate that an individual is being forced to act against his or her will.

**Espionage.** Overt, covert, or clandestine activity designed to obtain information relating to national defense with the intent that, or reason to believe that, it will be used to the injury of the United States or to the advantage of foreign nations.

**Exception—Physical Security.** Relief from compliance with a specific physical security standard or requirement.

**Explosive Ordnance Disposal (EOD).** The detection identification, field evaluation rendering-safe recovery and final disposal of unexploded ordnance, also known as bomb disposal.

**Facility—FAA.** Any manned or unmanned building, structure warehouse, appendage, storage area, utilities, and components, which, when related by function and location form an operating entity owned, operated, or controlled by the FAA.

**Facility Physical Security Management Plan (FPSMP).** A systematic, written plan intended to provide a concise analysis of a facility security program, to be used by the facility manager as an aid in effective utilization of his/her security resources.

**For Official Use Only (FOUO).** A term used to designate unclassified information which is to be protected against uncontrolled release. FOUO information is not a classification term; however, it is subject to the control and protection requirements of FAA Order 1600.15D. FOUO information may also be withheld from public disclosure under criteria established under the Freedom of Information Act, Title 5 U.S.C. Section 552a(b).

**Identification Media.** Badges, credentials, or other media used to establish identity of FAA employees, government officials, contractors, vendors, or the identity of individuals.

**Intrusion Detection System (IDS).** A combination of components, electronic and other types, that signal unauthorized attempts to enter or tamper with a protected area or object. IDS for use in FAA facilities must comply with the requirements of Federal Specification W-A-450-C, November 1991.

**Jurisdiction.** The limits within which an individual or agency has designated authority under the law.

**Key and Lock Control.** A formal method for identifying the location and accounting for the keys and locks in a facility.

**Object Protection.** Physical security and/or electronic safeguards that are dedicated to the protection of specific items such as a safe, file cabinet, room, or other defined area.

**Official Information.** Information that is owned by, produced by, or subject to the control of the U.S. Government.

**Physical Security.** That part of security concerned with the implementation of physical measures designed to safeguard personnel to prevent unauthorized access to activities, property, equipment, and classified or sensitive unclassified information and to safeguard them against sabotage, espionage, fraud, waste and abuse, and other threats.

**Physical Security Plan.** A detailed written plan for the disposition and utilization of physical security resources available to a facility. A physical security plan may be developed for a facility of any size, as opposed to a Facility Physical Security Management Plan (FPSMP) which is normally developed for larger facilities like ARTCC's.

**Physical Security Survey.** A comprehensive formal assessment of a facility's physical security program.

**Protective Barriers.** Physical or technical means to define the physical limits of a facility, operation, or area for the purpose of denying unauthorized access.

**Restricted Area.** A protected area established to control access or entry for purposes other than safeguarding classified information.

**Risk.** A measure of the potential degree of loss of protected information.

**Risk Analysis.** Method of quantifying the probability of loss or damage to an asset.

**Risk Assessment—Physical Security.** Utilization of risk analysis techniques to identify level of physical security countermeasures required for a facility, asset, or operation.

**Sabotage.** Any action performed with the intent that it will damage or destroy Government property or disrupt Government operations.

**Security Threat.** Any agency or condition, actual or potential, that can adversely impact a facility resulting in loss or damage to property, injury or loss of life, disruption of the mission of the facility, or a combination of these consequences.

**Standard—Physical Security.** A requirement, specification, or procedure established by directive that provides for uniform description, comparison, evaluation, and selection of physical security measures.

**Systematic Pilferer.** An individual who commits theft according to a preconceived plan.

**Technical Officer (TO).** The designated technical representative and direct interface between the contracting officer (CO), contractor, and program officer.

**Terrorism.** The unlawful use or threatened use of force or violence against individuals or property for the purpose of coercion or intimidation to achieve political, religious, or ideological goals.

**Threat.** The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operation.

**Threat Assessment.** An evaluation of the overall threat to a program activity system or operation.

**Vandalism.** Willful or malicious destruction, damage, or defacement of public and/or private property.

**Vulnerability.** Weakness in any aspect of an asset's design, use, mission, staffing, or other characteristic that if exploited would have an adverse impact on the security or operations of the asset.

**Vulnerability Analysis.** The process by which facilities operations, programs, or activities are examined to identify weaknesses susceptible to exploitation.

**Waiver.** Temporary relief from requirements to comply with a specific standard.

## **APPENDIX 2. OTHER STANDARDS, LAWS, DIRECTIVES, AND ORDERS THAT APPLY TO THE SAFEGUARDING OF FAA FACILITIES AND ASSETS UNDER THE PHYSICAL SECURITY MANAGEMENT PLAN**

### **SECTION 1. PROGRAM AUTHORITIES**

1. Title 41, United States Code (U.S.C.), Part 101, Management of Buildings and Grounds.
2. Section 301(a) of the Federal Aviation Act (FAAct) of 1958 (codified by Public Law (PL) 97-499, and now covered by 49 U.S.C. 106).
3. Section 303(d) of the FAAct of 1958 (codified by PL 97-499 and now covered by 49 U.S.C. 332, except that language in (d) after the semicolon is now covered by the last sentence of Section 307(b) of this Act (49 U.S.C. App 1348(b)).
4. Section 313(a) of the FAAct of 1958 (49 U.S.C. App 1354(a)).
5. Computer Security Act of 1987, PL 100-235.
6. The Federal Manager's Financial Integrity Act (FMFIA), PL 97-255.
7. Executive Order 12356, National Security Information.
8. Department of Transportation Physical Security Program Order DOT 1600.26A, dated July 25, 1990.
9. National Communications Security Instruction (NACSI), Number 4008, Safeguarding Communications Security (COMSEC) Facilities, National Security Agency.
- 10.-19. RESERVED.

### **SECTION 2. DOT/FAA ORDERS AND DIRECTIVES**

20. Within each of the following directives, there is specific guidance as to how the assets that are the subject of the directive are to be physically protected. When an asset is covered by one of the directives listed, the physical security safeguard requirements of the PSMP shall be the same as those prescribed in the applicable directive.
21. FAA Order 1000.32, Management Control Systems
22. FAA Order 1280.1, Protecting Privacy of Information About Individuals
23. FAA Order 1500.14, Travel Manual
24. FAA Order 1600.1, Personnel Security Program
25. FAA Order 1600.2, National Security Information
26. FAA Order 1600.8, Communications Security
27. FAA Order 1600.15, Control and Protection of "For Official Use Only Information"
28. FAA Order 1600.24, Use of Recording or Monitoring Equipment
29. FAA Order 1600.25, Identification Media, Passports and Credentials
30. FAA Order 1600.54, FAA Automated Information System Security Handbook
31. FAA Order 1600.55, Guidelines Procedures for Reporting Threats Against the President and Other Government Officials
32. FAA Order 1650.7, Civil Aviation Security Program Guidelines
33. FAA Order 1770.11, Mail Management Standards

**1600.6C**  
**Appendix 2**

34. FAA Order 1900.1, FAA Emergency Operations Plan
35. FAA Order 2770.4, Imprest Fund
36. 48 CFR 13.505-3, Standard Form 44 Purchase Order—Invoice Voucher (Procurements Under \$2,500)
37. FAA Order 4400.44, Standard Form 44 (SF-44) Purchase Order Invoice Voucher
38. FAA Order 4630.3, Survey of Lost, Damaged, or Destroyed Government Personnel Property
39. FAA Order 4650.21, Management In-Use Personal Property
40. FAA Order 4650.27, Acquisition and Distribution of Devices for the FAA Standard Key Lock System
41. FAA Order 4770.3, Transportation and Traffic Management
42. FAA Order 8080.1, Conduct of Airman Written Tests

4/16/93

1600.6C  
Appendix 3

## APPENDIX 3. FORMS AND REPORTS



4/16/93

1600.6C  
Appendix 3

## DEPARTMENT OF TRANSPORTATION

Part A—To Be Completed By Each Person Removing Equipment		Date
Name (Typed or printed)  _____ Typed or Printed  _____ Signature	Description of Equipment (Include serial number)	Owner <input type="checkbox"/> DOT <input type="checkbox"/> Personal <input type="checkbox"/> Vendor <input type="checkbox"/> Other (Specify) Return date _____
Property Custodian's Name (Printed), Rte. Symb., Telephone No. _____		Property Custodians Signature _____ Date _____

Part B—To Be Completed By DOT Personnel Only				
Organizational Element	Routing Symbol	Phone	Office Building	Room No.

Part C—To Be Completed By Non-DOT Personnel Only			
Employer	Address of Employer	DOT Official and Office Aware of Removal	Phone No.

Part D—To Be Completed By Guard		
Person removing property was— <input type="checkbox"/> DOT Employee <input type="checkbox"/> Other	If Other—Name of DOT official and office who verified removal	Verified by <input type="checkbox"/> Phone <input type="checkbox"/> In Person

Routing Instructions for Completed Forms		
<b>Guard:</b> Fold original with lower third exposed, staple, and forward to security office. Provide duplicate copy to individual concerned.		
<b>Security Office:</b> Forward to property management office.		
Routing of Completed Copies		
To	Routing Symbol	Organization
1		
2		

# Rules and Regulations Governing Public Buildings and Grounds

June 1991

## Federal Property Management Regulations Title 41, Code of Federal Regulations, Subpart 101-20.3

**Authority.** These rules and regulations are promulgated pursuant to Public Law 566, 80th Congress, approved June 1, 1948 (Title 40, U.S. Code 318); and the Federal Property and Administrative Services Act of 1949 (Title 63, United States Statutes at Large, 377), as amended.

**Applicability** (41 CFR 101-20.300). These rules and regulations apply to all property under the charge and control of the General Services Administration and to all persons entering in or on such property. Each occupant agency shall be responsible for the observance of these rules and regulations.

**Inspection** (41 CFR 102-20.301). Packages, briefcases, and other containers in the immediate possession of visitors, employees, or other persons arriving on, working at, visiting, or departing from Federal property, are subject to inspection. A full search of a person and any vehicle driven or occupied by the person may accompany an arrest.

**Admission to property** (41 CFR 101-20.302). Property shall be closed to the public during other than normal working hours. The closing of property will not apply to that space in those instances where the Government has approved the after-normal-working-hours use of buildings or portions thereof for activities authorized by Subpart 101-20.4. During normal working hours, property shall be closed to the public only when situations require this action to ensure the orderly conduct of Government business. The decision to close the property shall be made by the designated official under the Occupant Emergency Program after consultation with the buildings manager and the ranking representative of the Law Enforcement Branch responsible for protection of the facility or the area. The designated official is defined in § 101-20.003(g) as the highest ranking official of the primary occupant agency, or the alternate highest ranking official or designee selected by mutual agreement by other occupant agency officials. When property, or a portion thereof, is closed to the public, admission to this property, or a portion, will be restricted to authorized persons who shall register upon entry to the property and shall, when requested, display Government or other identifying credentials to the Federal Protective Officers or other authorized individuals when entering, leaving, or while on the property. Failure to comply with any of the above applicable provisions is a violation of these regulations.

**Preservation of property** (41 CFR 100-20.303). The improper disposal of rubbish on property; the willful destruction of or damage to property; the theft of property; the creation of any hazard on property to persons or things; the throwing of articles of any kind from or at a building or the climbing upon statues, fountains, or any part of the

building, is prohibited.

**Conformity with signs and directions** (41 CFR 101-20.304). Persons in and on property shall at all times comply with official signs of a prohibitory, regulatory, or directory nature and with the lawful direction of Federal Protective Officers and other authorized individuals.

**Disturbances** (41 CFR 101-20.305). Any loitering, disorderly conduct, or other conduct on property which creates loud or unusual noise or a nuisance; which unreasonably obstructs the usual use of entrances, foyers, lobbies, corridors, offices, elevators, stairways, or parking lots; which otherwise impedes or disrupts the performance of official duties by Government employees; or which prevents the general public from obtaining the administrative services provided on the property in a timely manner, is prohibited.

**Gambling** (41 CFR 101-20.306). Participating in games for money or other personal property or the operating of gambling devices, the conduct of a lottery or pool, or the selling or purchasing of numbers tickets, in or on property is prohibited. This prohibition shall not apply to the vending or exchange of chances by licensed blind operators of vending facilities for any lottery set forth in a State law and authorized by section 2(a)(5) of the Randolph-Sheppard Act (20 U.S.C. 107, et seq.).

**Alcoholic beverages and narcotics** (41 CFR 101-20.307). Operation of a motor vehicle while on the property by a person under the influence of alcoholic beverages, narcotic drugs, hallucinogens, marijuana, barbiturates, or amphetamines is prohibited. Entering upon the property, or while on the property, under the influence of or using or possessing any narcotic drugs, hallucinogens, marijuana, barbiturates, or amphetamines is prohibited. The prohibition shall not apply in cases where the drug is being used as prescribed for a patient by a licensed physician. Entering upon the property, or being on the property, under the influence of alcoholic beverages is prohibited. The use of alcoholic beverages on property is prohibited except, upon occasions and on property upon which the head of the responsible agency or his or her designee has for appropriate official uses granted an exemption in writing. The head of the responsible agency or his or her designee shall provide a copy of all exemptions granted to the buildings manager and the Chief, Law Enforcement Branch, or other authorized officials, responsible for the security of the property.

**Soliciting, vending, and debt collection** (41 CFR 101-20.308). Soliciting alms, commercial or political soliciting, and vending of all kinds, displaying or distributing commercial advertising, or collecting

private debts on GSA-controlled property is prohibited. This rule does not apply to (a) national or local drives for funds for welfare, health, or other purposes as authorized by 5 CFR, Parts 110 and 950, Solicitation of Federal Civilian and Uniformed Services Personnel for Contributions to Private Voluntary Organizations, issued by the U.S. Office of Personnel Management under Executive Order 12353 of March 23, 1982, as amended, and sponsored or approved by the occupant agencies; (b) concessions or personal notices posted by employees on authorized bulletin boards; (c) solicitation of labor organization membership or dues authorized by occupant agencies under the Civil Service Reform Act of 1978 (Pub. L. 95-454); and (d) leases, or its agents and employees, with respect to space leased for commercial, cultural, educational, or recreational use under the Public Buildings Cooperative Use Act of 1976 (40 U.S.C. 490(a)(16)). Public areas of GSA-controlled property may be used for other activities permitted in accordance with Subpart 101-20.4.

**Posting and distributing materials** (41 CFR 101-20.309). Posting or affixing materials, such as pamphlets, handbills, or flyers, on bulletin boards or elsewhere on GSA-controlled property is prohibited, except as authorized in § 101-20.308 or when these displays are conducted as part of authorized Government activities. Distribution of materials, such as pamphlets, handbills, or flyers, is prohibited, except in the public area of the property as defined in § 101-20.003(z), unless conducted as part of authorized Government activities. Any person or organization proposing to distribute materials in a public area under this section shall first obtain a permit from the building manager under Subpart 101-20.4 and shall conduct distribution in accordance with the provisions of Subpart 101-20.4. Failure to comply with those provisions is a violation of these regulations.

**Photographs for news, advertising, or commercial purposes** (41 CFR 101-20.310). Photographs may be taken in space occupied by a tenant agency only with the consent of the occupying agency concerned. Except where security regulations apply or a Federal court order or rule prohibits it, photographs for news purposes may be taken in entrances, lobbies, foyers, corridors, or auditoriums when used for public meetings. Subject to the foregoing prohibitions, photographs for advertising and commercial purposes may be taken only with written permission of an authorized official of the agency occupying the space where the photographs are to be taken.

**Dogs and other animals** (41 CFR 101-20.311). Dogs and other animals, except seeing eye dogs, other guide dogs, and animals used to guide or assist handicapped persons, shall not be brought upon

property for other than official purposes.

**Vehicular and pedestrian traffic** (41 CFR 101-20.312). (a) Drivers of all vehicles entering or while on property shall drive in a careful and safe manner at all times and shall comply with the signals and directions of Federal Protective Officers or other authorized individuals and all posted traffic signs. (b) The blocking of entrances, driveways, walks, loading platforms, or fire hydrants on property is prohibited; and (c) Except in emergencies, parking on property is not allowed without a permit. Parking without authority, parking in unauthorized locations or in locations reserved for other persons, or parking contrary to the direction of posted signs is prohibited. Vehicles parked in violation, where warning signs are posted, shall be subject to removal at the owners' risk and expense. This paragraph may be supplemented from time to time with the approval of the Regional Administrator by the issuance and posting of such specific traffic directives as may be required, and when so issued and posted such directives shall have the same force and effect as if made a part thereof. Proof that a motor vehicle was parked in violation of these regulations or directives may be taken as prima facie evidence that the registered owner was responsible for the violation.

**Explosives** (41 CFR 101-20.313). No person entering or while on property shall carry or possess explosives, or items intended to be used to fabricate an explosive or incendiary device, either openly or concealed, except for official purposes. (Weapons, see Title 18, U.S. Code Section 930.)

**Nondiscrimination** (41 CFR 101-20.314). There shall be no discrimination by segregation or otherwise against any person or persons because of race, creed, sex, color, or national origin in furnishing or by refusing to furnish to such person or persons the use of any facility of a public nature, including all services, privileges, accommodations, and activities provided thereby on the property.

**Penalties and other laws** (41 CFR 101-20.315). Whoever shall be found guilty of violating any rule or regulations in this Subpart 101-20.3 while on any property under the charge and control of the U.S. General Services Administration is subject to a fine of not more than \$50 or imprisonment of not more than 30 days, or both. (See Title 40, U.S. Code 318c.) Nothing in these rules and regulations shall be construed to abrogate any other Federal laws or regulations or any State and local laws and regulations applicable to any area in which the property is situated (Sec. 205(c), 63 U.S. Statutes, 390; 40 U.S. Code 486(c)).

# WARNING

## Title 18, United States Code, Section 930

## WEAPONS PROHIBITED

Federal law prohibits the knowing possession or the causing to be present of firearms or other dangerous weapons in Federal facilities and Federal court facilities by all persons not specifically authorized by Title 18, United States Code, Section 930(c). Violators shall be subject to fine and/or imprisonment for periods up to five (5) years.

## APPENDIX 4. OCCUPANT EMERGENCY PLAN--SAMPLE FORMAT

# Occupant Emergency Program

**M**ore than 900,000 people work in approximately 6,800 federally owned or leased Federal buildings. Countless visitors pass through these facilities each year. The U.S. General Services Administration (GSA) is the agency responsible for ensuring the safety and security of all of these people while they are on Federal property.

The Federal Property Management Regulations (FPMR) specifically require GSA to assist Federal agencies

who occupy these facilities in establishing and maintaining an Occupant Emergency Program (OEP). The FPMR defines an OEP as "... a short-term emergency response program [that] establishes procedures for safeguarding lives and property during emergencies in particular facilities."

An OEP has two components. The first is the development of procedures to protect life and property in federally occupied space under certain

emergency conditions. The second is the formation of an Occupant Emergency Organization within each agency, comprised of employees designated to undertake certain responsibilities and perform the specific tasks outlined in its OEP.

**NOTE:** The relevant sections of the FPMR are contained within the Appendix of this booklet.

## Occupant Emergency Plans

**T**his publication provides a step-by-step guide to assist Federal agencies in meeting FPMR occupant emergency requirements. As each agency completes development of an OEP, pertinent information should be published as a directive entitled *Occupant Emergency Plan for (Name of Facility)* and copies distributed to all individuals responsible for action in the event of an emergency.

The published Occupant Emergency Plan directive should contain a sign-off sheet, similar to the one on this page. Verification that those responsible for managing and performing tasks during an emergency is necessary to ensure that those individuals are aware of their responsibilities.

For small, one-level facilities, emergency information (telephone numbers, responsible individuals coordinators, etc.) may be entered on GSA Form 3415, Occupant Emergency Plan (abbreviated), shown on the following page. This form may not be used for facilities with more than 500 employees, unless its use is approved by the individual primarily responsible for the Occupant Emergency Program.

### Responsible Officials' Sign-Off Sheet

By their signatures below, the following officials verify that they have participated in the development of this Occupant Emergency Plan and fully understand the procedures to be followed in an emergency affecting the facility and employees for which they are responsible.

Designated Official: Name \_\_\_\_\_  
Signature \_\_\_\_\_  
Title \_\_\_\_\_

Building Manager: Name \_\_\_\_\_  
Signature \_\_\_\_\_

Tenant Agencies: Agency \_\_\_\_\_  
Ranking Official \_\_\_\_\_  
Signature \_\_\_\_\_  
Agency \_\_\_\_\_  
Ranking Official \_\_\_\_\_  
Signature \_\_\_\_\_  
Agency \_\_\_\_\_  
Ranking Official \_\_\_\_\_  
Signature \_\_\_\_\_

Physical Security Specialist: Name \_\_\_\_\_  
Signature \_\_\_\_\_

## APPENDIX 4. OCCUPANT EMERGENCY PLAN--SAMPLE FORMAT

### Responsibility

The FPMR places responsibility for managing emergencies in a federally owned or leased facility upon a "Designated Official," who is "... a designee selected by mutual agreement of occupant agency officials." (Section 101-20.003, Definitions). This person must supervise the development of the Occupant Emergency Plan and the staffing and training of the Occupant Emergency Organization.

### The Command Center

Emergency operations are directed from a Command Center. The Center should be centrally located and easily accessible for effective communication and control. A possible location would be the building's control center where the alarm panel is located. The Center should have good communications capability, including at least two telephones and, if possible, portable

radios and pagers. Messengers should be available to augment communications systems.

Provision should be made for an alternate Command Center, in case the main one is incapacitated, and for a Command Center at the site to which employees would be transferred if the facility has to be evacuated.

Include the location and telephone number for the Command Centers and alternate sites.

### Emergency Telephone Numbers

All personnel in the building should know who to contact in case of emergency. A list of emergency telephone numbers should be available to everyone. One way to ensure that everyone has and keeps a copy is to publish the list in the Federal telephone directory, preferably on the inside of the front cover or on the first page. The list also should be published with the Occupant Emergency Plan for the facility. Of course, it should be updated as assignments change.

### Building/Occupant Information

The Occupant Emergency Plan should contain specific information about the building's construction and its occupants in narrative form or on a Building Information Sheet and Occupant Information Sheet. Floor plans should be included, with evacuation routes clearly marked.

OCCUPANT EMERGENCY PLAN (Abbreviated)			DATE	
<i>(This form is provided as a suggested guide for storefront and/or ground level small office space)</i>				
AGENCY		MEDICAL ASSISTANCE		
FIRE	POLICE	OTHER PHONE		
FEDERAL PROTECTIVE SERVICE		BUILDING MANAGER		
OFFICIAL IN CHARGE		DUTY PHONE		
EMERGENCY ORGANIZATION INFORMATION (Coordinators, Monitors, and Bomb Search Officer)				
NAME	DUTY	OFFICE PHONE	OTHER PHONE	
1.				
2.				
3.				
4.				
EMERGENCY PLAN GUIDANCE				
Know Evacuation Routes		Know the Plan of Action		
FIRE OR SMOKE		BOMB THREAT		
1. Sound building alarm. 2. Call Fire Department 3. Notify Official in Charge 4. Notify Buildings Manager 5. Notify Federal Protective Service 6. Assist Fire Department. 7. Close windows and doors (Do no lock)		1. Record information on back of this form. 2. Notify Official in Charge 3. Notify Police 4. Notify Federal Protective Service 5. Notify Buildings Manager 6. Search immediate area and public areas for suspicious object. 7. If suspicious package or bomb found: a. Do not touch. b. Notify Bomb Squad c. Evacuate area.		
EARTHQUAKE				
1. Take cover under table, desk, or in doorway. 2. Do not run outdoors.				
SEVERE WEATHER		CIVIL DISTURBANCE		
1. Secure objects outside building. 2. Prepare to move to place of safety. 3. Stay away from large windows. 4. For tornado, open windows. 5. Know location of utility shutoff valves and switches. 6. Stay tuned to weather reports. 7. Standby for further instructions.		1. Notify official in charge. 2. Secure doors. 3. Notify Police 4. Notify Federal Protective Service 5. Notify Buildings Manager		
<b>NOTE: In all emergencies, be prepared to assist the handicapped.</b> <i>Bomb Threat Checklist on Reverse Side</i>				

Direct orderly flow of persons during fire drills and emergencies along prescribed routes, including orderly exit from the building at the first or ground floor.

- Ensure that all persons have vacated the floor.

### Area or Wing Monitors

- Work with floor monitor; notify floor monitor when area has been completely cleared.
- Ensure that evacuation routes are clearly identified and made known to occupants.
- Direct orderly flow of persons during drills and emergencies, along the prescribed evacuation routes.
- Ensure that area or wing is completely vacated, when required.
- Ensure that windows and doors are closed, lights on, and electrical appliances off during fire evacuations.
- Ensure that windows and doors are left open and light on during bomb threat evacuations.
- Supervise stairwell monitors and monitors for the handicapped; maintain list of handicapped persons, providing revisions to the floor monitor. (List should include name, telephone extension, room number, and type of handicap.)

## Stairwell Monitors

- Support the area/wing monitor.
- If evacuating because of a bomb threat, search stairwell.
- Control movement of persons on stairways, keeping them in single file and moving steadily at a walking pace; instruct persons to grasp handrails.
- Keep door open to stairway until the area/wing is clear.
- Restrict and monitor use of stairwells and escalators as necessary.
- Assign monitors for the handicapped, one per handicapped person.

Floor Team/\_\_\_\_\_ Floor (continued)  
(Elevator Monitors)

Combine a sheet of elevator monitor for each floor there elevator may not be captured. Buildings with automatic elevator capturing systems will need elevator monitors only for the floor where elevators are captured.

[illegible]

## Elevator Monitors

- Assist floor monitors.
- Be familiar with the provisions of GSA Bulletin FPMR D-198 covering emergency plans for using elevators to evacuate handicapped persons.
- Be familiar with manual operation of elevators.

# Communications

**O**f high-priority concern to members of the Occupant Emergency Organization are the primary and alternate means of communication that will be used (1) to activate the organization; (2) to inform building occupants of the nature of an emergency and what action to take; and (3) to coordinate activities during the emergency.

In some cases, the building's fire alarm system may be sufficient means of notifying the organization and the occupants. However, such a general alarm may not be available or appropriate, and telephones, public address systems, and/or messengers may prove more feasible. If telephones are used, a communications coordinator should be appointed to set up a system of contacting all members of the emer-

gency organization. This person could also be responsible for updating lists of telephone numbers.

Multilevel buildings may have emergency telephone systems for coordinating emergency activities. However, most buildings must rely on the normal telephone system, the public address system, the fire alarm, and messengers.

## Child Care Centers in Federal Facilities

**T**he designated official and a physical security specialist should work with the director of a child care center in a Federal facility to develop and post emergency response procedures. Center staff should know whom to contact in the event of a medical emergency, how the center

will be notified of a fire or other danger that may require evacuation, the location of fire alarm boxes and fire extinguishers, the primary and secondary evacuation routes, and the locations of safe areas.

Each staff member should be assigned

a specific group of children for whom he or she is to be responsible during an emergency. Center staff should conduct practice drills over the prescribed evacuation routes so children will not be unprepared or unduly alarmed should a real emergency occur.

## Responsible Officials' Sign-Off Sheet

By their signatures below, the following officials certify that they have participated in the development of this Occupant Emergency Plan and fully understand the procedures to be followed in an emergency affecting the facility and employees for which they are responsible.

**Designated Official:**

Name \_\_\_\_\_

Signature \_\_\_\_\_

Title \_\_\_\_\_

**Building Manager:**

Name \_\_\_\_\_

Signature \_\_\_\_\_

**Tenant Agencies:**

Agency \_\_\_\_\_

Ranking Official \_\_\_\_\_

Signature \_\_\_\_\_

Agency \_\_\_\_\_

Ranking Official \_\_\_\_\_

Signature \_\_\_\_\_

Agency \_\_\_\_\_

Ranking Official \_\_\_\_\_

Signature \_\_\_\_\_

Agency \_\_\_\_\_

Ranking Official \_\_\_\_\_

Signature \_\_\_\_\_

**Physical Security Specialist:**

Name \_\_\_\_\_

Signature \_\_\_\_\_

## Emergency Telephone Numbers

Building Command Center \_\_\_\_\_

Alternate \_\_\_\_\_ Off-site \_\_\_\_\_

Building Manager \_\_\_\_\_

Fire Department \_\_\_\_\_

**Police:**

Federal Protective Service \_\_\_\_\_

Local Police Department \_\_\_\_\_

**Bomb Disposal:**

Military \_\_\_\_\_

Local Police \_\_\_\_\_

**Hazardous Materials Information:**

**CHEMTREC: 800-424-9300 (from Washington, DC, 483-7616)**

(Also list numbers of state and local agencies, local number for Environmental Protection Agency, and poison control centers.)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Utilities:**

Gas \_\_\_\_\_

Electric \_\_\_\_\_

Water \_\_\_\_\_

Telephone \_\_\_\_\_



## Building Information Sheet

Building name \_\_\_\_\_

Building number \_\_\_\_\_

Address \_\_\_\_\_

Year building completed \_\_\_\_\_

Type of construction \_\_\_\_\_

Number of floors \_\_\_\_\_

Mezzanine(s) \_\_\_\_\_

Basement(s) \_\_\_\_\_

Gross floor areas \_\_\_\_\_ square feet

Net assignable floor area \_\_\_\_\_ square feet

Government occupied floors \_\_\_\_\_

Other Tenants \_\_\_\_\_

Fire alarm system and signals \_\_\_\_\_

Automatic sprinkler system \_\_\_\_\_

Voice communications systems \_\_\_\_\_

<b>OCCUPANT EMERGENCY PLAN (Abbreviated)</b> (This form is provided as a suggested guide for storefront and/or ground level small office space)				DATE	
AGENCY			AGENCY		
FIRE		POLICE		MEDICAL ASSISTANCE	
FEDERAL PROTECTIVE SERVICE			BUILDING MANAGER		OTHER PHONE
OFFICIAL IN CHARGE			DUTY PHONE		
<b>EMERGENCY ORGANIZATION INFORMATION</b> (Coordinators, Monitors, and Bomb Search Officer)					
NAME		DUTY		OFFICE PHONE	OTHER PHONE
1.					
2.					
3.					
4.					
<b>EMERGENCY PLAN GUIDANCE</b>					
Know Evacuation Routes			Know the Plan of Action		
<b>FIRE OR SMOKE</b>			<b>BOMB THREAT</b>		
1. Sound building alarm. 2. Call Fire Department _____ 3. Notify Official in Charge _____ 4. Notify Buildings Manager _____ 5. Notify Federal Protective Service _____ 6. Assist Fire Department. 7. Close windows and doors (Do no lock)			1. Record information on back of this form. 2. Notify Official in Charge _____ 3. Notify Police _____ 4. Notify Federal Protective Service _____ 5. Notify Buildings Manager _____ 6. Search immediate area and public areas for suspicious object. 7. If suspicious package or bomb found: a. Do not touch. b. Notify Bomb Squad _____ c. Evacuate area.		
<b>EARTHQUAKE</b>					
1. Take cover under table, desk, or in doorway. 2. Do not run outdoors.					
<b>SEVERE WEATHER</b>			<b>CIVIL DISTURBANCE</b>		
1. Secure objects outside building. 2. Prepare to move to place of safety. 3. Stay away from large windows. 4. For tornado, open windows. 5. Know location of utility shutoff valves and switches. 6. Stay tuned to weather reports. 7. Standby for further instructions.			1. Notify official in charge. 2. Secure doors. 3. Notify Police _____ 4. Notify Federal Protective Service _____ 5. Notify Buildings Manager _____		
<b>NOTE: In all emergencies, be prepared to assist the handicapped.</b> <i>Bomb Threat Checklist on Reverse Side</i>					

<b>TELEPHONE BOMB THREAT CHECKLIST</b> <b>Important: REMAIN CALM</b>		CODE NUMBER
<b>SECTION I — INSTRUCTIONS</b>		
1. Follow instructions received from your supervisor, Federal Protective Officer, or the designated official.	2. If you are ordered to evacuate, take with you any drafts, forms, or reports you may have prepared regarding the threat.	
<b>SECTION II — PERTINENT DATA</b>		
1. TIME BOMB IS SET TO EXPLODE  _____ a.m.                      _____ p.m.	4. LOCATION OF BOMB a. Building _____ b. Floor _____ c. Area _____	
2. DESCRIBE TYPE OF BOMB  _____ _____	5. EXPLAIN WHY CALLER WISHES TO INJURE OR KILL INNOCENT PERSONS  _____ _____	
3. DID CALLER INDICATE KNOWLEDGE OF THE FACILITY? <input type="checkbox"/> NO <input type="checkbox"/> YES (Explain) _____		
<b>SECTION III — DESCRIPTION OF CALLER'S VOICE</b>		
<input type="checkbox"/> MALE <input type="checkbox"/> FEMALE <input type="checkbox"/> YOUNG <input type="checkbox"/> OLD <input type="checkbox"/> MIDDLE-AGED <input type="checkbox"/> CALM <input type="checkbox"/> NERVOUS <input type="checkbox"/> REFINED <input type="checkbox"/> ROUGH <input type="checkbox"/> ACCENT <input type="checkbox"/> SPEECH IMPEDIMENT  (Describe) _____	_____ _____ _____ _____	
DO YOU RECOGNIZE VOICE? <input type="checkbox"/> NO <input type="checkbox"/> YES (Whose voice is it?) _____		
<b>SECTION IV — BACKGROUND NOISE</b>		
<input type="checkbox"/> TRAFFIC <input type="checkbox"/> HORNS <input type="checkbox"/> WHISTLES <input type="checkbox"/> MUSIC <input type="checkbox"/> BELLS <input type="checkbox"/> AIRCRAFTS <input type="checkbox"/> TAPE RECORDER NERVOUS <input type="checkbox"/> MACHINERY	<input type="checkbox"/> RUNNING MOTOR (Type) _____ <input type="checkbox"/> OTHER _____	
<b>SECTION V — TELEPHONE LINE DATA</b>		
1. LINE ON WHICH CALL WAS RECEIVED <input type="checkbox"/> LISTED NUMBER? <input type="checkbox"/> UNLISTED NUMBER?		
2. IS THIS A NIGHT NUMBER? <input type="checkbox"/> YES (Whose number?) _____		
3. HAS A BOMB THREAT CALL BEEN PREVIOUSLY RECEIVED ON THIS NUMBER? <input type="checkbox"/> NO <input type="checkbox"/> - YES (Explain) _____		
<b>SECTION VI — REPORTING OF THREAT</b> <b>Caution: DO NOT TALK TO OTHERS about Incident.)</b>		
1a. NAME OF PERSON RECEIVING CALL  _____	2. REPORT THREAT TO: a. FEDERAL PROTECTIVE SERVICE DIVISION	
b. DIVISION AND TELEPHONE NUMBER  _____	b. DESIGNATED OFFICIAL  _____	
c. TIME AND DATE CALL RECEIVED  _____	c. BUILDINGS MANAGER  _____	

## Building Information Sheet

Building name \_\_\_\_\_

Building number \_\_\_\_\_

Address \_\_\_\_\_

Year building completed \_\_\_\_\_

Type of construction \_\_\_\_\_

Number of floors \_\_\_\_\_

Mezzanine(s) \_\_\_\_\_

Basement(s) \_\_\_\_\_

Gross floor areas \_\_\_\_\_ square feet

Net assignable floor area \_\_\_\_\_ square feet

Government occupied floors \_\_\_\_\_

Other Tenants \_\_\_\_\_

Fire alarm system and signals \_\_\_\_\_

Automatic sprinkler system \_\_\_\_\_

Voice communications systems \_\_\_\_\_

Begin with the lowest floor and work upward. Because agencies move, this sheet must be reviewed and updated accordingly.

Total occupancy \_\_\_\_\_

Page 11

## Command Center Team

(Update as necessary and check quarterly)

Building \_\_\_\_\_

Address \_\_\_\_\_

**Designated Official:**

\_\_\_\_\_

Title

\_\_\_\_\_

Name of incumbent

\_\_\_\_\_

Telephone: Office

\_\_\_\_\_

Home

**Occupant Emergency Coordinator:**

\_\_\_\_\_

Title

\_\_\_\_\_

Telephone: Office

\_\_\_\_\_

Home

**Floor Team Coordinator:**

\_\_\_\_\_

Title

\_\_\_\_\_

Name of incumbent

\_\_\_\_\_

Telephone: Office

\_\_\_\_\_

Home

**Floor Team—Floor \_\_\_\_\_**

Complete one sheet per floor. Modify the sheet to correspond to your building's unique layout. In particular, appoint as many area and stairwell monitors as your building requires.

Floor Monitor \_\_\_\_\_

Title \_\_\_\_\_

Telephone \_\_\_\_\_

Skills \_\_\_\_\_

Area \_\_\_\_\_ Monitor \_\_\_\_\_

Title \_\_\_\_\_

Telephone \_\_\_\_\_

Skills \_\_\_\_\_

Area \_\_\_\_\_

Title \_\_\_\_\_ Monitor \_\_\_\_\_

Telephone \_\_\_\_\_

Skills \_\_\_\_\_

Stairwell \_\_\_\_\_ Monitor \_\_\_\_\_

Title \_\_\_\_\_

Telephone \_\_\_\_\_

Skills \_\_\_\_\_

Stairwell \_\_\_\_\_ Monitor \_\_\_\_\_

Title \_\_\_\_\_

Telephone \_\_\_\_\_

Skills \_\_\_\_\_

**Monitors for the Handicapped**

\_\_\_\_\_  
Monitor

\_\_\_\_\_  
Handicapped person/handicap

\_\_\_\_\_  
Monitor

\_\_\_\_\_  
Handicapped person/handicap

\_\_\_\_\_  
Telephone

\_\_\_\_\_  
Telephone

\_\_\_\_\_  
Telephone

\_\_\_\_\_  
Telephone

## Evacuation Information

### Person Authorized To Order Evacuation

Designated Official \_\_\_\_\_

Occupant Emergency Coordinator \_\_\_\_\_

Federal Protective Service Official \_\_\_\_\_

Building Manager \_\_\_\_\_

Fire Department Official in Charge \_\_\_\_\_

### Evacuation Signals

**Fire:** Describe method of notification for complete or partial evacuation.

---

---

---

---

**Explosion or Gas Leak:** Describe method of notification for complete or partial evacuation.

---

---

---

---

**Suspicious Object:** Describe method of notification for complete or partial evacuation.

---

---

---

---



## Evacuation/Bomb Search Chart

Building \_\_\_\_\_ Date \_\_\_\_\_

Floor/Area	TIME		Remarks
	Evacuated	Searched	

**NOTE:** This chart provides a useful tool for reviewing the effectiveness of an evacuation and/or search. Remarks may include who searched the floor or area, where persons were relocated, and any unusual circumstances.

# Management Regulations

## Part 101-20. Management of Buildings and Grounds (Only relevant parts are included)

### 101-20.003. Definitions

(g) The "Designated Official" is the highest ranking official of the primary occupant agency of a Federal facility; or, alternatively, a designee selected by mutual agreement of occupant agency officials.

(i) The term "emergency" includes bombings and bomb threats, civil disturbances, fires, explosions, electrical failures, loss of water pressure, chemical and gas leaks, medical emergencies, hurricanes, tornadoes, floods, and earthquakes. The term does not apply to civil defense matters such as potential or actual enemy attacks. Note: Civil defense emergencies are addressed by the Federal Emergency Management Agency.

(v) "Occupant Emergency Organization" means the emergency response organization comprised of employees of Federal agencies designated to perform the requirements established by the Occupant Emergency Plan.

(w) "Occupant Emergency Plan" means procedures developed to protect life and property in a specific Federally-occupied space under stipulated emergency conditions.

(x) "Occupant Emergency Program" means a short-term emergency response program. It establishes procedures for safeguarding lives and property during emergencies in particular facilities.

### 101-20.103. Physical protection and building security

#### 101-20.103-1. Standard protection

For properties under its custody and control, GSA will provide standard protection services by:

(g) Coordinating a comprehensive Occupant Emergency Program.

#### 101-20.103-4. Occupant Emergency Program

(a) The Designated Official (as defined in 101-20.003(g)) is responsible for developing, implementing, and maintaining an Occupant Emergency Plan (as defined in 101-20.003(w)). The Designated Official's responsibilities include establishing, staffing, and training an Occupant Emergency Organization with agency employees. GSA shall assist in the establishment and maintenance of such plans and organizations.

(b) All occupant agencies of a facility shall fully cooperate with the Designated Official in the implementation of the emergency plans and the staffing of the emergency organization.

(c) GSA shall provide emergency program policy guidance, shall review plans and organizations annually, shall assist in training of personnel, and shall otherwise ensure proper administration of Occupant Emergency Programs (as defined in 101-20.003(x)). In leased space GSA will solicit the assistance of the lessor in the establishment and implementation of plans.

(d) In accordance with established criteria, GSA shall assist the Occupant Emergency Organization (as defined in 101-20.003(v)) by providing technical

personnel qualified in the operation of utility systems and protective equipment.

#### 101-20.103-5. Initiating action under Occupant Emergency Programs

(a) The decision to activate the Occupant Emergency Organization shall be made by the Designated Officials, or by the designated alternate official. Decisions to activate shall be based upon the best available information, including an understanding of local tensions, the sensitivity of target agency(ies), and previous experience with similar situations. Advice shall be solicited, when possible, from the GSA buildings manager, from the appropriate Federal Protective Service Official, and from Federal, State, and local law enforcement agencies.

(b) When there is immediate danger to persons or property, such as fire, explosion, or the discovery of an explosive device (not including a bomb threat), occupants shall be evacuated or relocated in accordance with the plan without consultation. This shall be accomplished by sounding the fire alarm system or by other appropriate means.

(c) When there is advance notice of an emergency, the Designated Official shall initiate appropriate action according to the plan.

(d) After normal duty hours, the senior Federal Official present shall represent the Designated Official or his/her alternates and shall initiate action to cope with emergencies in accordance with the plans.

# Occupant Emergency Plan Check List

If you can't check any of the following questions, your Occupant/Emergency Plan needs strengthening. Contact your building manager and/or the GSA Physical Security and Law Enforcement Office nearest you if you need help.

- |   |  |   |
|---|--|---|
| <input type="checkbox"/> Did an advisory committee of appropriate officials (Building Manager, Federal Protective Service, etc.) assist in developing the plan? Is this committee still available for consultation? | <input type="checkbox"/> Have all occupants been told how to get first aid/CPR fast?                                 | <input type="checkbox"/> In leased space, is the responsibility of the owner/lessor clearly defined? If contract guards are used, have their authority and responsibilities been defined? |
| <input type="checkbox"/> Has an emergency organization been established, preferably following existing lines of authority?  | <input type="checkbox"/> Do occupants know what to do if an emergency is announced?                                  | <input type="checkbox"/> Are floor plans and occupant information readily available for use by police, fire, bomb search squads, and other emergency personnel?                           |
| <input type="checkbox"/> Are emergency organization members designated by position rather than by person?   | <input type="checkbox"/> Are evacuation procedures established and familiar to all employees?                        | <input type="checkbox"/> Has a hazard communication program been implemented in accordance with 29CFR 1910.1200?  |
| <input type="checkbox"/> Do organization members know their own responsibilities as well as who has decisionmaking authority in any given situation?  | <input type="checkbox"/> Have special procedures been established for evacuation of the handicapped?                 | <input type="checkbox"/> Has an inventory been compiled of all hazardous materials used in individual workplaces and stored anywhere in the building?                                     |
| <input type="checkbox"/> Has a procedure been established to notify organization members?   | <input type="checkbox"/> Are fire-reporting procedures established and familiar to all employees?                    | <input type="checkbox"/> Are emergency telephone numbers displayed and/or published where they are readily available? Are they reviewed and updated frequently?                           |
| <input type="checkbox"/> Are emergency procedures easy to implement rapidly?  | <input type="checkbox"/> Have firefighting plans been developed which coordinate internal and external resources?    |   |
| <input type="checkbox"/> Has a Command Center location been established?  | <input type="checkbox"/> Do occupants know to whom they should report an unlawful act? Any other emergency incident? |   |
| <input type="checkbox"/> Are communications at the Command Center adequate?   | <input type="checkbox"/> Do employees know what procedures to follow if they receive a telephone bomb threat?        |   |
| <input type="checkbox"/> Do emergency organization members know under what circumstances they are to report to the Command Center?  | <input type="checkbox"/> Are bomb search responsibilities and techniques specified in the plan?                      |   |
| <input type="checkbox"/> Are employees who do not have assigned duties excluded from the Command Center?  | <input type="checkbox"/> Are procedures established for reporting the progress of a search, evacuation, etc.?        |   |
| <input type="checkbox"/> Are emergency telephone numbers posted in the Command Center and throughout the building? Published in the telephone book?   | <input type="checkbox"/> Have procedures been established for bomb disposal?   |   |
| <input type="checkbox"/> Are procedures established for handling serious illness, injury, or mechanical entrapment?   | <input type="checkbox"/> Have emergency shutdown procedures been developed?  |   |
| <input type="checkbox"/> Do organization members know what medical resources are available and how to reach them?   | <input type="checkbox"/> Have plans been made for capture and control of elevators?                                  |   |
|   | <input type="checkbox"/> Have arrangements been made for emergency repair or restoration of services?                |   |
|   | <input type="checkbox"/> Have drills and training been adequate to ensure a workable emergency plan?                 |   |

## GSA Law Enforcement Offices

### Central Office

Office of Physical Security and Law  
Enforcement (PS)  
General Services Administration  
18th and F Sts., NW.  
Room 2314  
Washington, DC 20405

### National Capital Region

Washington, DC, and nearby  
Maryland and Virginia  
Federal Protection Division (WPS)  
Southeast Federal Center  
3rd and M Streets, SE.  
Building, 159E, Second Floor  
Room 211  
Washington, DC 20407

### Region 2

New York, New Jersey, Puerto Rico,  
Virgin Islands  
Law Enforcement Branch (2PML)  
26 Federal Plaza, Room 17-130  
New York, NY 10278

Maine, Vermont, New Hampshire,  
Massachusetts, Rhode Island,  
Connecticut

Law Enforcement District  
(2PML-XL)  
Tip O'Neill Building  
10 Causeway Street, Room 108  
Boston, MA 22222

### Region 3

Pennsylvania, Delaware, Maryland  
Virginia, West Virginia  
Law Enforcement Branch (3PML)  
Robert N.C. Nix Federal Building  
and U.S. Post Office  
9th and Market Sts. Room 3345  
Philadelphia, PA 19107

### Region 4

North Carolina, South Carolina,  
Georgia, Tennessee, Alabama,  
Mississippi, Florida, Kentucky  
Law Enforcement Branch (4PML)  
Summit Building  
401 West Peachtree, Suite 2500  
Atlanta, GA 30365

### Region 5

Ohio, Michigan, Wisconsin, Indiana,  
Illinois, Minnesota  
Federal Protection Division (SPS)  
230 South Dearborn Street  
Room 3540  
Chicago, IL 60604

### Region 6

Kansas, Missouri, Iowa, Nebraska  
Law Enforcement Branch, (6PML)  
1500 East Bannister Road  
Room 2137  
Kansas City, MO 64131

### Region 7

Texas, Louisiana, Arkansas,  
Oklahoma, New Mexico  
Law Enforcement Branch (7PML)  
819 Taylor Street, Room 14A14  
Fort Worth, TX 76102

Colorado, Utah, Wyoming, Montana,  
North Dakota, South Dakota  
Law Enforcement District (7PXML)  
Denver Federal Center, Building 1  
Denver, CO 80225

### Region 9

California, Arizona, Nevada, Hawaii,  
Guam, Northern Mariana Islands  
Law Enforcement Branch (9PML)  
525 Market Street, 30th Floor  
San Francisco, CA 94105

Washington, Oregon, Idaho, Alaska  
Law Enforcement District (9PX-3L)  
916 Second Ave., Room 2610  
Seattle, WA 98174

## APPENDIX 5. PERIMETER CONTROLS

1. **OBJECTIVE.** To establish physical security standards for perimeter fence and gate construction.

### SECTION 1. FAA STANDARD SECURITY FENCE

#### 2. GENERAL REQUIREMENTS.

a. **Siting.** Whenever locations permit, fencing shall be located not less than 50 feet (15.2 meters) or more than 200 feet (61 meters) from the object of protection.

b. **Clear zone requirement.** To the extent that is possible, fencing shall be constructed so that an unobstructed area or clear zone is maintained on both sides of the barrier.

c. **Grounding requirement.** Fencing shall be grounded in accordance with requirements of FAA-STD-019.

3. **FABRIC.** Fences, including gate structures, shall be of Number 9-gauge or heavier chain link fabric. Fabric shall be aluminum or zinc-coated steel wire chain link with mesh openings not larger than 2 inches (5.08 centimeters) on a side (FAA Specification FAA-E-2065). The top and bottom edges of the fence fabric shall be twisted and barbed.

a. **Fabric ties.** Fence fabric shall be attached to the exterior side of line posts using not less than 9-gauge steel ties. If the ties are coated or plated, the coating or plating will be electrolytically compatible with the fence fabric to inhibit corrosion. Ties will be spaced not more than 14 inches (0.025 meters) apart.

b. **Height.** The standard height of an FAA security fence shall be 8 feet (2.4 meters). This includes a fabric height of 7 feet (2.1 meters) plus a top guard extension of 1 foot (0.304 meters). The distance between the bottom of the fence fabric and firm packed ground shall not exceed 2 inches (5.08 cm).

c. **Stretcher bars.** Fence fabric shall be attached to terminal posts with stretcher bars 0.25 inches by 0.75 inches, which engage each fabric link. The stretcher bars shall be held to the fence post with clamps in such a way as to hold the fabric taut. The clamps for the stretcher bars shall be placed within 4 inches (0.12 meters) of the top and bottom rail, and shall be spaced not more than 14 inches (0.42 meters) apart. The bolts securing the clamps to the posts shall be peened or otherwise modified in a manner approved by the SSE to deter attempts at unauthorized removal.

4. **TOP GUARD.** A top guard is required on all FAA standard chain link security fences and gates. The top guard shall:

a. Face outward and upward at an angle of 45 degrees from the horizontal.

b. Have support arms that are constructed of Number 12-gauge pressed steel, permanently affixed to the top of the fence posts by riveting or other approved method, to increase the overall height of the fence by a minimum of 1 foot (0.304 meters).

c. Have support arms that must be so constructed and secured to the fence post that they will withstand an actual test pull down of a vertical load of 250 pounds without sagging or bending.

d. Have 3 strands of 12-gauge barbed wire with 4-point barbs spaced 4 inches (0.1 meter) apart and stretched taut between the support arms.

e. Have the top strand of barbed wire 12 inches (0.304 meters) above and parallel to the fence line, with the remaining 2 strands spaced uniformly between the top of the fence fabric and the top strand.

5. **REINFORCEMENT.** Taut reinforcing wires a minimum of 9-gauge shall be installed and interwoven with or affixed with 12-gauge fabric ties spaced 12 inches (0.304 meter) apart along the top and bottom of the fence fabric.

6. **FENCING POSTS AND HARDWARE.** All fence posts, supports, and hardware for FAA security fences shall meet the requirements of Federal Specification RR+F-191J/GEN of July 1981.

a. All fastening and hinge hardware shall be secured against attempts at unauthorized removal by peening or other method approved by the SSE so as to allow proper operation of the components but deter disassembly of fence sections or removal of gates.

b. All posts and structural supports shall be located on the interior of the fence. Posts shall be spaced not more than 6 feet (1.8 meters) apart and shall be embedded in bell shaped concrete footings to a depth of 2 feet (0.61 meters) to prevent shifting or sagging.

7. **CULVERTS AND TROUGHS.** Where the perimeter fence traverses culverts, troughs, ditches, or other openings greater than 96 square inches (0.06 square meters) in area, the opening shall be protected by an extension of the fence

construction. This extension may consist of iron grills or other barrier structures of a design approved by the SSE for the purpose of preventing unauthorized access.

a. Bars and grills shall be installed in such a way that they do not impede required drainage.

b. Hinged security grills used with an approved high security hasp, shackle, and padlock, which can be opened when necessary, are often a workable solution to securing drainage structures.

## 8. GATES.

a. Construction. Security fence gates shall be constructed of a galvanized tubular steel framework. The following requirements apply:

(1) The steel used in the framework shall have a minimum outside diameter of 2 inches (0.06 meter) and a weight per linear foot of not less than 2.75 pounds.

(2) Framework shall be trussed to limit sagging and provide additional strength.

(3) Large gates shall have horizontal and vertical support members of the same type and size as the outside network.

(4) Fabric used for gate construction shall be of the same type and quality specified for the remainder of the fence and shall be attached in the same manner.

(5) Hardware used on swing gates shall have the securing bolts peened or otherwise modified in a manner approved by the SSE to deter their unauthorized removal.

(6) Bolts used on sliding gates which hold the trolley wheels in place shall be modified by peening or spot welding to make unauthorized removal difficult.

(7) Ground clearance. The space between the bottom edge of the gate and the pavement or firm ground shall not exceed 2 inches (0.03 meters). Where the gate is situated over a sharply graded street as is often found with vehicular gates, excessive gaps can occur beneath the gate. In addressing this problem, the SSE will provide the facility manager with appropriate guidance for meeting the security standard of 2 inches. Some approaches include the use of cantilevered or overhead gate structures which are recessed into sub-surface troughs or provision of an extension on the bottom edge of swinging gates which can be lowered into a slotted channel extending beneath ground level when the gate is closed.

9. GATE LOCKS. The locking mechanism for a gate shall be installed on the inside. The following requirements apply:

a. The lock shall be protected with steel shields to prevent tampering with the mechanism from outside the gate.

b. Eye bolts can be welded to the fence frame and gate posts when necessary to permit secure locking.

c. Use of a chain and padlock shall be avoided whenever possible, because the chain permits an excessive distance between single gates and the gate posts, and between the frame of double gates. In those instances where it is determined that a chain and padlock is the only feasible solution to securing a gate structure, the facility manager shall consult with the SSE to determine the specific installation and control requirements.

## 10. SPECIAL REQUIREMENTS.

a. Gates over 6 feet (1.83 meters) in height shall have locks at the top and bottom to ensure that the gate cannot be pried a sufficient distance to allow unauthorized entry.

b. Vehicular gates. Vehicular gates should be set well back from the public highway or access road in order that temporary delays caused by identification control checks at the gate will not cause undue traffic congestion. Sufficient space shall be provided at the gate to allow for spot checks, inspections, searches, and temporary parking of vehicles without impeding traffic flow.

c. PIDS. Usually gates are protected by the use of locks and intermittent patrol checks or by fixed posts. The use of PIDS devices at gate entrances has to be justified on the basis of identified need. If the gate is used only intermittently, or if additional protection is desired for the gate portion of the facility perimeter fence line, the use of PIDS may be considered either separately or in combination with other devices. Among the various devices that can be employed for controlling access at gate entrances are electronic card access devices, cipher locks, and CCTV.

d. CCTV either in the surveillance mode or in the motion-sensing mode of operation can be very useful in physical security operations and is frequently used within the Federal Government to serve as an admittance verification and control or to verify an alarm condition in support of other sensors. These functions are served by placing CCTV cameras in critical locations with direct visual monitoring capability from a remote vantage point or security control center (SCC).

(1) CCTV may be used on gates that are not manned continuously. This system consists of a CCTV camera, monitor, and associated electrical and communications circuitry. The camera is remotely controlled by the monitoring personnel (security guard force) at the SCC. CCTV on gates shall include the use of a two-way communication system between the monitor panel in the SCC and the protected gate access point. With this capability, the person in the SCC can communicate with the person seeking entry and, after verifying his or her authority to enter, can remotely release the gate lock.

(2) Controls for CCTV shall be enclosed in metal housing and properly secured to prevent any tampering by unauthorized personnel.

## APPENDIX 6. LIGHTING

1. **OBJECTIVE.** To establish physical security standards for perimeter and critical area lighting.

### SECTION 1. PROTECTIVE LIGHTING

2. **DESIGN OBJECTIVE.** The cone of illumination from lighting units shall be directed downward and away from the structure or area being protected and away from security personnel assigned to provide such protection. The lighting shall be so arranged as to create a minimum of shadows and a minimum of glare in the eyes of guards.
3. **STANDOFF REQUIREMENTS.** Lighting units for a perimeter fence shall be located a sufficient distance within the protected area and above the fence so that the light pattern on the ground will include an area on both the inside and outside of the fence. The distance between each perimeter light pole and the perimeter fence is termed "standoff." For design purposes, the standoff will be between 20 feet (6 meters) and 35 feet (11 meters). The standoff area shall be as flat as possible and kept free of vegetation. Generally, the light band should illuminate the fence barrier and extend as deeply as possible into the approach area.

#### 4. PHYSICAL SEPARATION OF MOUNTING

**POLES.** The distance between poles used to mount luminaries along the perimeter shall not exceed four times the mounting height. (e.g., If the perimeter lighting luminaire is mounted on a support pole at a vertical height of 20 feet (6 meters) from the ground, the separation between any two adjacent poles shall not be greater than 80 feet (24 meters)).

5. **LOCATION OF MOUNTING POLES.** Perimeter lighting mounting poles shall be located inside the perimeter fence and meet standoff requirements specified in paragraph 3.

### SECTION 2. LIGHTING SYSTEMS

6. **GENERAL.** There are four general types of protective lighting systems. Making the determination as to which system is appropriate for a given application will depend upon the overall security environment and the requirements of the facility concerned.

7. **CONTINUOUS LIGHTING.** This is the most commonly used form of protective lighting systems and the type that is specified for FAA facilities. It consists of a series of fixed luminaries arranged to illuminate a given area on a continuous basis with overlapping cones of light during the hours of darkness. The two primary methods of employing continuous lighting are:

- a. **Glare projection.** This type of lighting is useful where the glare of lights directed toward the exterior of the facility and into the eyes of a potential intruder is the desired effect. At FAA facilities, the lighting at gate entrance locations is an example on one application of this method. A vehicle approaching the gate during the hours of darkness is fully illuminated, but the guard station remains in the shadow of the light pattern.

- b. **Controlled lighting.** This method is used most often at FAA locations where it is necessary to limit the width of the lighted strip outside the perimeter fence because of nearby residential areas, public thoroughfares, or other activity

centers. In controlled lighting, the width of the illuminated strip can be controlled and arranged as required. For instance, one possible configuration might be to have a wide band of illumination inside the fence and a much more narrow band on the exterior of the fence. The design of the luminaire permits directing the light source to achieve these results. The angle of the luminaries is primarily downward with some angle adjustment to attain the desired bandwidth.

- c. **Surface lighting.** Addresses those lighting systems that are used to provide required levels of illumination for critical areas and structures.

8. **STANDBY LIGHTING.** The arrangement of this system is similar to the continuous lighting array. The difference is that the luminaries are not continuously lighted during hours of darkness but are activated manually or automatically when suspicious activity is detected by the security force or IDS.

9. **MOVABLE LIGHTING.** This type of lighting consists of manually operated movable light sources and luminaries, often searchlights, which may be lighted during hours of darkness to cover specific areas as needed. Movable lights are normally used to supplement continuous or standby systems.



**10. EMERGENCY LIGHTING.** This system may duplicate the other three systems in whole or in part. Its use is normally limited to periods of main power failure or other emergencies. Security lighting at FAA facilities should be connected to the emergency power system. Emergency lighting depends on alternative power sources such as portable generators or batteries.

**11. INCANDESCENT LAMPS.** These are common glass light bulbs in which the light is produced by the resistance of a filament to an electric current. Special purpose bulbs are manufactured with interior coatings to reflect the light, with built-in lenses to direct or diffuse the light, or the naked bulb can be enclosed in a shade or luminaire fixture to accomplish the same results.

a. **Advantages:** Instant start, good light control, good color rendition, and lowest initial cost.

b. **Disadvantages:** High operating costs, short lamp life (500-2000 hours), 20 lumens per watt.

**12. MERCURY VAPOR.** These lamps emit a blue-green light caused by an electric current passing through a tube of conducting and luminous gas. They are more efficient than incandescent lamps of comparable wattage and are in widespread use for interior and exterior lighting, especially where people are working.

a. **Advantages:** Long lamp life, 50 lumens per watt, low operating cost compared to incandescent.

b. **Disadvantage:** Limited light control (beam spread or pattern), high initial cost, does not restart immediately after power failure.

**13. SODIUM VAPOR.** Sodium vapor lamps are constructed on the same general principle as mercury vapor lamps but emit a golden yellow glow. They are more efficient than the other two types and are used where the color is acceptable, such as on streets, roads, and bridges. These lamps can be color corrected by using special lenses.

a. **Advantages:** Good light pattern control, long lamp life, 103 lumens per watt.

b. **Disadvantages:** Higher initial cost. Not suitable on applications where process color rendition is critical, but some lamps are designed to be color-corrected.

**14. METAL HALIDE.** These types of lamps emit a harsh yellow-colored light. They employ sodium, thallium, indium, and mercury.

a. **Advantages:** Moderately long lamp life, 71 lumens per watt, natural colored light, low operating costs.

b. **Disadvantages:** High initial cost, does not restart immediately after power failure.

#### **15. FLUORESCENT LAMPS.**

These are large, elongated bulbs which provide a high light output and have a recoverage light life of 7,500 hours. They have a higher initial cost than incandescent lamps, but a lower operating cost.

a. **Advantages:** Moderately long lamp life, 67 lumens per watt, low operating cost, even lighting from lamp with no hot spots.

b. **Disadvantages:** Higher initial cost than incandescent. Light control suitable for general areas, large fixture is required, light output is sensitive to ambient temperatures.

### **SECTION 4. GENERAL SPECIFICATIONS**

#### **16. PERIMETER LIGHTING.**

a. The perimeter is considered to be the FAA installation property line unless a fence barrier exists in which case the fence will be considered the perimeter.

b. Fenced perimeters are classified as follows:

(1) **Isolated fenced perimeters** are fence lines around areas where the fence is 100 feet (31 meters) or more from buildings or operating areas, and where the approach area is clear of obstruction for 100 or more feet outside the fence and is not used by other personnel. In general, both glare projection and controlled illumination are acceptable for these perimeters. In either case, patrol roads and paths should be kept unlighted whenever possible.

(2) **Semi-isolated fence perimeters** are fence lines where approach areas are clear of obstruction for 60 to 100 feet (18 to 31 meters) outside the fence and the general public or installation personnel seldom have reason to be in this area. Patrol roads and paths should be kept in relative darkness whenever possible.

(3) **Non-isolated fence perimeters** are fence lines immediately adjacent to operating areas within the installation, other installations, or public thoroughfares where outsiders or installation personnel may move about freely in the approach area. The width of the lighted strip in this case will depend upon the relative clear zone inside and outside the fence. Under these conditions it may not be practicable to keep the patrol area dark.

**17. BUILDING FACE PERIMETERS.** These consist of faces of buildings which are on or within 20 feet (6 meters) of the property line or area line to be protected, and where the public may approach the buildings. Guards may be stationed inside or outside the building. Doorways or other insets in the building's face should receive special attention for lighting to eliminate shadows.

**18. AREAS AND STRUCTURES.** Critical assets and structures to be protected within the perimeter may consist of yards, storage spaces, large open working areas, microwave towers, and other sensitive areas and structures. Security lighting requirements should be determined using the following guidelines:

**a. Open yards and outdoor storage areas.**

(1) The illumination of open yards and storage areas adjacent to a perimeter (between guards and fences) should be in accordance with the illumination requirements for the remainder of the perimeter. Where lighting is deemed necessary in other open yards, the illumination should not be less than 0.2 footcandle at any point.

(2) Lighting units shall be placed in outdoor storage areas to provide an adequate distribution of light in aisles, passageways, and recesses to eliminate shadowed areas where unauthorized persons could conceal themselves.

**b. Critical structures and areas** shall be the first consideration in designing protective fencing and lighting. Power, heat, water, communications, flammable materials, critical storage areas, delicate machinery, areas where confidential or sensitive material is stored or produced, and valuable finished products need special attention.

(1) Critical structures or areas which are classified as vulnerable from a distance should be kept dark (standby lighting available), and those which can be damaged close at hand should be well lighted.

(2) The surrounding areas shall be well-lighted to force a potential intruder to cross a light area, and the walls (if a building) shall be lighted to a height of 8 feet (2.44 meters) to facilitate silhouette vision.

**19. POWER SOURCES.** Usually the primary power source at an FAA facility will be a local public utility. As FAA security control seldom extends beyond the perimeter, the interest of the security planner and guard force begins where the powerfeeder lines enter the installation. Protective and security lighting should, wherever possible, be tied into the facility emergency power system, so that in the event of a failure of the public power, the protective lighting will continue to function.

**20. WIRING SYSTEMS.** Both multiple and series circuits may be utilized in a protective lighting system, depending upon the type of luminaire used and other design features of the system. The circuit should be arranged so that failure of any one lamp will not leave a large portion of the perimeter fence or a major segment of a critical or vulnerable asset in darkness.

a. Connections shall be such that normal interruptions caused by overloads, accidents, fire, or other emergencies will not interrupt the protective system.

b. Feeder lines shall be located underground.

**21. LUMINAIRES.** The term luminaire refers to the combination of light source reflector and housing. Luminaries selected for perimeter lighting systems shall be roadway style units unless otherwise specified and approved by ACO-300. In addition, the following apply:

a. **Design.** Luminaries shall be of a design which permits directing the light toward the base of the fence to provide a zone of illumination at least 3 feet (0.9 meters) in width on both sides of the fence.

b. **Coverage Pattern.** Failure of a single luminaire for whatever reason shall not result in total loss of visibility for that section of the perimeter. The lights shall be installed so that the cones of illumination overlap.

**22. ILLUMINATING VERTICAL SURFACES.** When lighting vertical surfaces, such as the walls of a building, the luminaire units will be installed so that they are set back from the surface to be illuminated a distance equivalent to at least 1/4 of the height of the luminaire.

**23. POWER.** FAA protective lighting systems shall be connected to an uninterrupted power supply (UPS) (emergency power) source whenever possible. Where backup power is available for a perimeter lighting system, it should be capable of switching automatically to full load within 60 seconds.

**24. GATE ENTRANCE ILLUMINATION.**

a. **Attended entrances.** Perimeter lighting at manned entrances shall be adequate to identify persons, inspect vehicles, and prevent anyone from slipping unobserved into or out of the premises.

b. **Unattended entrances.** Semi-active and unmanned entrances shall have the same degree of continuous lighting as the remainder of the perimeter except that additional, standby lighting will be available to provide the same illumination required for manned entrances when the entrance becomes active.

c. Lighting intensity at entrances shall be planned to ensure that an arriving driver can readily recognize the premises and see where to drive his or her vehicle. Normally, for pedestrian and vehicle entrances, this controlled illumination level should extend for a distance of 25 feet (8 meters) on either side of the entrance.

**25. ILLUMINATION REQUIREMENTS FOR GUARD HOUSES.** Lighting inside guard houses should be controlled so that guard functions cannot be readily observed.

## APPENDIX 7. BUILDING CONTROLS

### SECTION 1. DOORS

1. **GENERAL.** Door construction is important as a primary safeguard against unauthorized access to buildings and structures. These standards are to be used by the SSE and facility manager alike to assist them in establishing appropriate safeguards.

2. **DOOR AND FRAME CONSTRUCTION.** Doors and frames shall be of substantial metal or solid wood construction.

a. If a wooden door is not of solid core construction or contains panels that are less than 1-3/4 inches thick, it can be reinforced on the inside with at least 16-gauge sheet steel attached with security screws to provide additional protection if required.

b. Heavy-duty builders hardware shall be used throughout.

3. **HINGES.** Hinges shall be located on the inside of the door, concealed, or otherwise installed so as to be inaccessible from the exterior side when the door is closed.

a. If this is not possible, the hinges shall be installed so they cannot be removed by taking out the screws or so they will withstand the use of a chisel or similar cutting device.

b. The hinge pins in exterior mounted hinges shall be welded, flanged, or otherwise modified in a manner approved by the SSE to prevent their removal.

4. **DOORS WITH GLASS PANELS.** It is not uncommon to find existing door structures that have glass panels as part of the door. The ability of a door to resist attempts at forcible entry is greatly reduced when this situation occurs. Glass panels can be broken and the resulting opening used to access the locking mechanism.

a. The most effective solution to an entrance door with glass panels is to replace the entire door with a solid wood or metal door structure. This is not always possible; therefore, alternatives must be considered.

b. Glass panels in doors can be protected by using wire mesh (number 9 gauge, 2-inch square mesh) or steel bars.

(1) Steel bars shall be at least 0.5 inch (1.25 centimeter) round, or 1-inch (2.5 centimeter) by 0.25-inch (0.63 centimeters) flat steel material, spaced not more than 5 inches (13 centimeters) apart.

(2) The spacing of the bars will depend on the type and accessibility of the locking mechanism.

(3) Iron and steel grills of at least 0.13 inch (0.33 centimeter) material of 2-inch mesh are also acceptable.

(4) If either mesh or bars are used they shall be securely fastened to the inside of the door so that they cannot be pried loose. Mesh or bars shall be installed on the interior of the door using round headed bolts that are thoroughly bolted to the frame.

5. **ROLLING OVERHEAD DOORS.** Rolling overhead doors that are not controlled or locked by electric power shall be protected by slide bolts on the bottom bar. Chain-operated doors should be provided with a cast iron keeper and pin for securing the hand chain. For crank operated doors, the physical security measures taken must prevent unauthorized use of the door either by immobilizing the crank or locking the door to the frame with padlocks or both.

6. **SOLID OVERHEAD, SWINGING, SLIDING, OR ACCORDION TYPE DOORS.** This type of door shall be secured with a high security cylinder lock or a high security padlock, in conjunction with a metal slide bar, bolt, or deadbar on the inside.

7. **METAL ACCORDION GRATE OR GRILL TYPE DOORS.** This type of door shall have a secure metal guide track at the top and bottom and be provided with a high security cylinder lock or padlock which will provide the necessary protection.

### SECTION 2. WINDOWS

8. **GENERAL.** Window openings, like doors, can be inviting targets for potential intruders. They also can serve as a means for removing U.S. Government property and documents from a facility. Windows, like doors, have an

aesthetic value, and when considering security safeguards, these concerns must be addressed. Fire and safety concerns also must be coordinated by the SSE when considering measures that would affect window openings. Any part of a

window that is 18 feet (5 meters) or less above ground, or 18 feet (5 meters) or less from a potential access point such as an adjoining building, tree, etc., shall be considered as vulnerable to access.

**9. CONSTRUCTION.** Windows shall be of sturdy construction and properly set into substantial frames. The window frame must be securely fastened to the building so that it cannot be pried loose and the entire window removed.

**a. If a window can be opened, it shall be secured on the inside.** The mechanism used to secure the window may be a bolt, a slide bar, or crossbar. Key-operated locking devices for windows shall be coordinated with and approved by the appropriate fire and safety officials before installation.

**b. Hardware.** Outside hinges on a window shall be of the security type or be welded, flanged, or otherwise modified to make unauthorized removal difficult.

**10. WINDOW GLASS.** As with glass panels in a door, window glass can be broken or cut to enable an intruder to reach inside and release the lock.

**a. When determined necessary to provide the required degree of safeguarding, bars or steel grills may be used to protect vulnerable window openings.**

**b. Prior coordination with fire and safety officials shall be accomplished before placing bars or any other type of obstruction across window openings that might impede evacuation efforts in the event of a fire or other emergency.**

**11. STEEL BARS AND GRILLS,** when used, shall be installed on the inside of the window opening, wherever possible, to ensure maximum protection.

**a. Bars** shall be at least 0.5 inches (1.25 centimeters) in diameter if they are round and at least 1 inch (2.5 centimeters) wide by 0.25 inches (0.63 centimeters) thick if they are of the flat type.

**b. Grills** shall be constructed of Number 9-gauge security mesh, with individual mesh square dimensions not to exceed 2 inches on a side.

**c. Bars and grills** must be securely fastened to the window frame so that they cannot be pried loose.

**12. GLASS BRICK.** Glass brick may be used as a substitute for conventional windows provided that its use meets ventilation requirements and in conformance with fire and safety regulations.

**13. GLASS AND STEEL FRAMEWORK.** Small glass squares set in steel framework cannot be considered as secure construction. An intruder can break a pane of glass and reach through the opening to access the locking mechanism. The metal portion is normally not intended to provide protection against forced entry and is vulnerable to breaking or cutting by a potential intruder.

### SECTION 3. MISCELLANEOUS OPENINGS

**14. MANHOLES.** Many FAA facilities have manholes which provide entrances into the buildings for service purposes. Others may provide access to utility tunnels containing pipes for heat, gas, water, telephone transmission conduits, cables, and other utilities.

**a. Manhole covers on FAA property must be secured if they provide access to an FAA building or to any communications or other utility lines servicing that building or operation.**

**b. A chain and high security padlock can be used to secure a manhole cover.** The use of a hinged steel deadbar secured with a high security padlock and hasp is another alternative method for securing manhole covers.

**15. ACCESSIBLE STEEL GRATES AND DOORS.**

Grates and doors on ground level are other potential access points into a facility. These types of openings often serve as service entrances or exterior elevator entrances, or they may simply provide light and air to the basement level of the building. If the mounting frame is properly secured, the grates or doors can be welded into place, or they can be secured with a steel chain and high security padlock.

**16. SEWERS AND STORM DRAINS.** These features shall be secured if the areas of the openings associated with them are larger than 96 square inches (0.06 square meters).

**17. ROOFTOP ACCESS POINTS.** Rooftop structures can present readily available points of access to a potential intruder. An advantage of accessing a building from the roof is that an intruder can often work without the risk of detection once he or she has gained access to the roof area. Openings in elevator penthouses, roof top hatchways, and trap doors are sometimes omitted from a building's safeguarding plan because they are not often used.

**a. Roof top access points shall be secured by locks, bars, etc., and shall be inspected by the SSE during the conduct of each survey and inspection of the facility.**

**b. Skylights and similar structures shall be protected in the same way prescribed for window openings—with steel bars or mesh. Such protection shall, if possible, be installed inside the opening to make it more difficult to remove.**

**18. TRANSOMS** may appear to be small, but they must not be overlooked as points of potential access. A simple solution may be to seal the transom permanently. However, if this is not possible, each transom should be locked from the inside with a sturdy sliding bolt lock or other similar device, or be equipped with steel bars or grills installed on the inside.

**19. VENTILATING SHAFTS, VENTS, OR DUCTS,** as well as openings in the building wall that accommodate exhaust fans and similar appliances, represent possible points of access. A ventilating shaft or duct may be large enough to permit a potential intruder access into the building from the exterior. Securing openings of this type will require provision of effective man-barriers that will deter physical access while at the same time not interfere with the flow of air in the case of ventilating apertures. Normally, the use of steel bars set into a sturdy frame affixed to the duct or vent wall will provide the needed safeguard. Bars provide less impediment to air flow than security mesh or screens.

## APPENDIX 8. SECURITY GUARD FORCE

### SECTION 1. INTRODUCTION

1. **PURPOSE.** To establish minimum standards for the selection and utilization of contract security guards for FAA facilities.

#### 2. CONTRACT SECURITY REQUIREMENTS.

a. **Manager of the Office or Facility** submitting a request for guard services or for renewing existing guard services shall ensure that the statement of work and the request for bid are coordinated with the SSE as a must reviewer prior to submission to the contracting office.

b. **Manager of the FAA Contracting Office** responsible for advertising bids, reviewing bids, and selecting the contractor shall ensure that the standards contained in the sections that follow are incorporated into any FAA contract for security guard services.

### SECTION 2. RESPONSIBILITIES

3. **GENERAL.** The contract security guard force at an FAA facility is to serve as management's representative in the administration and enforcement of the facility physical security program. To do this effectively, each member of the guard force must understand his or her role and responsibilities. Initial guard force training standards must be clearly specified in the statement of work and in the contract for services.

4. **RESPONSIBILITIES.** The following are general duties and responsibilities that are assigned to the contract guard force. These responsibilities shall be reviewed by the SSE and the facility manager and added to or modified as appropriate for inclusion in the statement of work and request for bid for security guard services for each facility.

a. **Guard and protect** all public and private property within your jurisdiction to include material, equipment, supplies, and buildings against damage, theft, fire, trespass, or sabotage.

b. **Guard and protect** all Government classified or sensitive information, documents, material, and equipment within your jurisdiction from unauthorized access or theft.

c. **To the extent prescribed** by established orders, policies, and procedures, operate, maintain, and enforce the system of personnel identification and access control for facility employees and visitors.

d. **Consistent with authority,** apprehend and detain all suspicious persons, or those who gain unauthorized access to the facility for release to local law enforcement authorities.

e. **Maintain law and order,** and prevent illegal acts which jeopardize the safety and security of the facility and its personnel.

f. **Conduct periodic patrols** of the facility grounds and buildings. Note any security deficiencies and report them in an expeditious manner to designated FAA or supervisory personnel.

g. **Make appropriate watch clock station checks** if required.

h. **Enforce the facility rules and regulations** governing control of all vehicular and personnel traffic entering the facility.

i. **Maintain key control and accountability** for facility keys issued to guard force.

j. **Report all violations of rules, regulations, and security procedures** to the contracting officer's technical representative (COTR) or his designated representative.

k. **In an emergency,** follow existing emergency and contingency operating procedures.

l. **Enforce the established policies and procedures** for controlling the removal of property and documents from the facility.

m. **Respond to protective alarm signals,** investigate and report any suspicious activity in accordance with established security policies and procedures.

n. **Provide written and verbal reports** as required by governing policies and procedures.

o. **Perform escort duties** as required by security policies and procedures for the facility.

### SECTION 3. GUARD QUALIFICATIONS

#### 5. PURPOSE.

Individual guard qualifications are based on the needs of the U.S. Government, in general, and the FAA, in particular. The following basic qualifications shall apply to any individual being considered for employment or assignment as a security guard at an FAA facility:

a. **U. S. citizenship.** Guard force personnel assigned to duties at FAA facilities shall, without exception, be U. S. citizens.

b. **Personal traits.** The statement of work, request for bid, and any contract between the FAA and a provider of security guard services shall make it clear that each security guard assigned to duties at an FAA facility will be expected to possess the following characteristics:

(1) Ability to exercise good judgment.

(2) Ability to interact with people in a positive manner.

(3) Ability to maintain a high level of performance.

c. **Professional training.** Before contract security guards are allowed to assume duties at an FAA facility the contracting officer or his/her designated representative shall require positive evidence that each individual concerned has undertaken, and has documentation reflecting, successful completion of the specific security guard training program requirements that may be mandated by the state and local civil jurisdictions in which the FAA facility is located.

d. **Education.** Prior to acceptance for duty at an FAA facility, the contracting officer shall require positive evidence from the security guard contractor that each guard has a minimum of a high school education. Evidence of satisfactory completion of a General Education Development (GED) examination at the high school level is acceptable. In addition, honorable military or police experience is desirable.

e. **Writing skills.** Each individual assigned as a security guard at an FAA facility shall be able to understand and to speak English fluently and shall be able to prepare accurate written reports in English.

f. **Physical traits.** Prior to any contract security guard assuming duties at an FAA facility, the contracting officer shall require positive evidence from the security guard contractor that the individual has been medically examined by a licensed medical doctor and determined to be physically fit for duty within the preceding 30 days. The examination shall cover, as a minimum, the following:

(1) An evaluation as to whether the individual is in good general health, without any physical defects or abnormalities which would interfere with job performance.

(2) A determination that the individual is free of any communicable disease.

(3) A determination that the individual possesses binocular vision correctable to 20/30 (Snellen) and is not color blind.

(4) A test of hearing capability to determine if the individual is able to hear normal conversation at 20 feet and whispered conversation at 10 feet without the benefit of a hearing aid.

(Note: If state or local medical qualification standards for security guards are higher than those indicated above, the state and local standards shall apply.)

6. **PHYSICAL FITNESS REPORT.** The contractor shall be required to provide written certification of the physical fitness as outlined above. The written certification shall be accompanied by a report of medical examination conducted prior to entrance on duty and annually thereafter.

7. **AGE.** To be considered for appointment as an FAA contract guard, each individual must be at least 21 years of age at the time of employment.

### SECTION 4. ARMED GUARDS

8. **GENERAL.** In addition to meeting the requirements of this appendix, contract guards who are required to carry firearms shall comply with the provisions pertaining to the safeguarding and use of firearms by contract guard personnel as specified in Appendix 9. Contractors will provide the FAA contracting officer with certification that they carry not less than \$300,000 liability insurance.

9. **FIREARMS QUALIFICATION.** The contractor shall certify to the FAA contracting officer in writing that each contract guard authorized to carry a firearm at an FAA facility has successfully completed an FAA-approved firearms training course and has qualified with the firearm to be issued prior to entrance on duty.

10. **PROFICIENCY CERTIFICATION.** Firearms proficiency certification for contract guard personnel shall consist of supervised and recorded test course scoring under



the control of a certified firearms instructor. (Instructor certification may be from a Federal agency or a state law enforcement training agency.) The contractor shall be required to provide to the FAA contracting officer in writing the results of each proficiency test. Proficiency certification shall include the following:

a. The guard must achieve, annually, a minimum qualifying score with his/her issued firearm, on a recognized Federal, state, or National Rifle Association Firearms course.

b. Each guard must possess and demonstrate a thorough knowledge of firearms safety precautions during the annual certification process.

## SECTION 5. SUITABILITY INVESTIGATION

**11. GENERAL REQUIREMENT.** The private contractor providing security guard personnel for assignment to an FAA facility shall be required to certify in writing to the FAA contracting officer that each guard has successfully passed a preemployment suitability investigation before the guard is assigned to the FAA facility.

**12. SCOPE OF INVESTIGATION.** The private security guard contractor shall be required to conduct or have conducted a suitability-type investigation for each individual to be assigned security guard duties at an FAA facility. The investigation shall include the following:

a. Search of police and credit files in the area of residence.

b. Inquiries of former employers, fellow employees, listed and developed references, and schools attended.

**13. RESULTS OF INVESTIGATION.** The private security guard contractor shall provide copies of investigative reports for each contract guard to be employed by the FAA or a certified summary thereof to the FAA contracting officer prior to the individual's entrance on duty. The contracting officer may disapprove an individual if the contractor's investigation is incomplete or fails to provide evidence of the guard's suitability for performing guard duties specified herein.

**14. CLASSIFIED CONTRACT CLEARANCES.** In the case of a classified contract, the contractor guards must be cleared by the Defense Industrial Security Clearance Office (DISCO), based on an investigation conducted by the Defense Investigative Service (DIS).

## SECTION 6. GUARD FORCE INSTRUCTIONS

**15. GENERAL REQUIREMENT.** Instructions to the guard force will be issued in writing by the FAA office exercising managerial control over the security guard force. Instructions to the guard force issued by the security guard contractor will be approved by the FAA contracting officer's technical representative (COTR).

**16. GUARD ORDERS.** Instructions shall be in the form of general, special, and temporary orders. They should be clear and concise and should correctly and fully describe the duties and actions that the security guard is to carry out under specified conditions. The FAA COTR will be responsible for ensuring that such orders are maintained and are current.

a. **GENERAL ORDERS.** General orders are those which concern the guard force as a whole and are applicable at all posts and patrols. They will cover such items as wearing of the uniform, reporting for duty, report writing, etc.

b. **SPECIAL ORDERS.** Special orders prescribe the responsibilities of a particular post or patrol. Each post or patrol will have special orders issued concerning the location, duties, hours manned, etc.

c. **TEMPORARY ORDERS.** Temporary orders are issued for a short period covering a special or temporary situation. If it can be predetermined, temporary orders will indicate the period of time for which they are valid.

**17. CONTRACTOR RESPONSIBILITY FOR GUARD MANUAL.** Each contractor shall be required to develop and issue a current and comprehensive guard manual to each security guard assigned to duty on an FAA facility. The manual shall be coordinated with the FAA COTR and the servicing security element before issuance. The manual will contain the basic guidance issued by the contractor to its employees concerning matters of dress, discipline, patrolling,

first aid, emergency responsibilities, apprehension of suspects and arrest powers, courtesy, communications, chain of command, etc.

## SECTION 7. OPERATIONAL PLANNING

**18. GENERAL.** In developing an operational plan which includes provision of contract security guard services, there are basic concerns which shall be addressed. This section lists some of the areas that will be considered when determining the type, number, and organization of security guards required for a given facility.

### 19. STRATEGIC PLANNING CONCERNS.

- a. Existing and potential security hazards.
- b. Personnel and vehicle controls required for the facility.
- c. Sensitivity of the facility based on type of operations conducted or type of information and/or material present.

- d. The criticality of the facility.
- e. Dollar value of facility and cost of replacement.
- f. Mechanical security aids employed at the facility or which could be employed at the facility.
- g. Existence of large quantities of highly volatile liquids within the facility or immediately adjacent thereto.
- h. Vulnerability of the facility to outside risk factors.
- i. Size of the facility to be protected.
- j. Condition of the perimeter barriers and their relationship to contiguous areas.

## SECTION 8. TRAINING

**20. GENERAL REQUIREMENT.** At a minimum, guard force personnel will receive training in the security and security-related subjects listed in this section.

a. **CARE OF FIREARMS.** Guards will comply with all firearms certification and proficiency training requirements in accordance with this section and Appendix 11.

b. **USE OF FIREARMS.** Weapons will be used only in extreme emergency requiring the protection of life and then only in accordance with the requirements of Appendix 11.

c. **JURISDICTION AND AUTHORITY.** Training sessions shall include descriptions of the guard forces' responsibilities and authority with respect to apprehension, search, seizure, and use of deadly force.

d. **FIRST AID.** Guard Force personnel will be qualified in first aid and cardio pulmonary resuscitation.

e. **EMERGENCY RESPONSIBILITIES.** The guard force shall demonstrate proficiency in the use of emergency equipment such as fire extinguishers and water hoses.

f. **ORDERS.** The guard force will be able to demonstrate knowledge of the facility's general, temporary, and special orders.

g. **SECURITY AND CONTINGENCY SITUATIONS.** The guard force will be able to recognize and appropriately react to emergency situations involving sabotage, terrorism, hostage situations, and hijackings.

h. **SAFETY.** The guard force will be able to demonstrate general knowledge of the safety requirements for the facility with special emphasis on any volatile materials stored within the confines of the facility.

i. **FACILITY ACCESS CONTROL PROCEDURES.** Training will incorporate facility guidelines and procedures for personnel and vehicle access control.

j. **COMMUNICATIONS.** Training will address and allow guard personnel to demonstrate the proper use of primary, alternative, and emergency communications equipment.

k. **REPORTS.** Training will address and allow the guard personnel to demonstrate adequate report writing skills associated with security guard force operations.

## SECTION 9. SUPERVISION

**21. GENERAL REQUIREMENT.** The guard contract shall require the private security guard contractor to provide a qualified supervisor to oversee each security guard duty shift.

**22. WATCH CLOCK SYSTEM.** FAA facilities employing security guard forces shall provide a watch clock system or some type of electronic guard tour system to serve as a supervisory control and check on the performance of guard personnel.

**23. ADDITIONAL SUPERVISORY CONTROLS.** The FAA contract shall identify specific procedures and requirements for periodic guard reporting to supervisory personnel by the use of radio, telephone, or hand-held radio.

**24. SHIFT CHECK REQUIREMENT.** The contract for security guard services shall require the contractor to have a qualified supervisor personally check guard performance at least one time during each security guard shift.

## SECTION 10. CONTRACTS REQUIRING A FACILITY CLEARANCE (DD-254)

**25. GENERAL REQUIREMENT.** FAA contracts for private security guard services must be in compliance with DD-254 (Facility Clearance) requirements. The paragraphs in this section shall be added to the guard contract.

**26. CONTRACTOR REQUIREMENT.** The contractor will give his/her personal superintendence to the work or will supervise all personnel required to perform the required services through a designated full-time supervisory representative, satisfactory to the contracting officer.

**27. CONTRACTOR SUPERVISORY REPRESENTATIVE.** The contractor's supervisory representative will have had experience in security plant protection at a level commensurate with the work scope of this contract and will be of unquestionable integrity and ability and able to pass a background investigation. The supervisory representative will:

a. Inspect each guard shift before posting and periodically during the shift to observe the conduct of the guards from the standpoint of efficiency, conduct, and compliance with guards' regulations and instructions.

b. Enter each inspection and the results thereof in the guard log.

c. Have the entry signed by the contractor supervisory representative.

**28. PERFORMANCE CRITERIA.** In making the required supervisory inspection, the contractor will determine at a minimum that the guard is in uniform when carrying out the duties and responsibilities of the FAA contract. The inspection shall ensure that the overall appearance and demeanor of the guard is one that promulgates professionalism, not only during the actual inspection but throughout the assigned shift.

a. The contractor shall ensure each post of duty has an up-to-date copy of the regulations and instructions pertaining to the guard post and a copy of the contract guard handbook is immediately available at each post of duty.

b. The guard has studied and is thoroughly familiar with the regulations and instructions and is aware that he/she must comply with them at all times. This can be verified by asking questions during the inspection.

## SECTION 11. GUARD FORCE EQUIPMENT

**29. GENERAL REQUIREMENT.** FAA shall require that the contractor providing security guard services to an FAA facility provide all necessary equipment required by the security guard to perform his or her duties in a competent, capable, and efficient manner.

**30. EQUIPMENT REQUIREMENTS.** Minimum guard force equipment requirements include the following:

a. All guard force personnel will wear prescribed uniforms. Deviations are not acceptable other than those that may be necessary in the interest of health and safety. High standards of personnel appearance will be maintained.

b. The FAA contract shall stipulate that private security guards be either armed or unarmed. If the contract requirements call for the guard to be armed, the standard

weapon shall be either a .38 caliber revolver or a 9mm semi-automatic pistol of American manufacture to be provided by the guard contractor.

c. The use of privately owned weapons or munitions while on duty will not be authorized.

d. Guards will be provided with communications equipment that is appropriate for them to use in carrying out their assigned duties. Equipment will include radio transceivers, telephones, and intercoms as deemed appropriate.

e. Equipment such as the following will also be made available to guards: first aid kits, high power flashlights, key control containers, portable fire extinguishers, traffic control devices, and such other items as management may deem necessary.

**31. USE OF SENTRY DOGS.** Careful planning, to include legal guidance, will be effected in considering the acquisition and employment of sentry dogs at agency facilities.

## APPENDIX 9. KEY AND LOCK CONTROL PROCEDURES

### 1. ISSUANCE AND CONTROL OF LOCKS AND

**KEYS.** An effective lock and key issuance and control system is essential to the safeguarding of property and controlling access. For effective control, accurate records shall be maintained and dated and semi-annually physical inspections and inventories made. Keys shall be stamped "Do Not Duplicate" prior to being issued.

**2. KEY CONTROL OFFICIAL.** A key control official shall be appointed in writing for every FAA facility having control over its own locking system. This official is responsible for the supply of locks and how they are stored; the handling of keys; records maintenance; investigation of lost keys; inventories and inspections; custody of master keys and control keys, if applicable; regulations concerning locks and keys at the facility; maintenance and operation of the facility's key depository; and the overall supervision of the key program at the facility.

**3. RECORD REQUIREMENTS.** The key control official shall maintain a permanent record of the following:

**a. Locks by number, showing:**

- (1) The location of each lock.
- (2) The key combination, (i.e., pin lengths and positions).
- (3) Date of last key change.

**b. Keys by number, showing:**

- (1) Location of each key.
- (2) Type and key combination of each key.
- (3) A record of all keys not accounted for.

### 4. ISSUANCE AND CONTROL PROCEDURES.

**a. Keys, coded cards, and push-button combinations** shall be accessible only to those persons whose official duties require access to them.

**b. Combinations to push-button locks** shall be changed following the discharge, suspension, or reassignment of any person having knowledge of the combination and at such other times as deemed appropriate.

**c. Issuance of keys** shall be kept to a minimum and take place under constant key control supervision. The following requirements apply:

- (1) Unissued keys shall be stored in a locked container when not in use.
- (2) Access lists for persons authorized to draw keys shall be maintained in the key storage container.
- (3) Key containers shall be checked periodically and all keys accounted for on a semi-annual basis.
- (4) Keys must be retrieved from personnel transferred, discharged, suspended, or retiring.

### 5. LOST AND UNACCOUNTED FOR KEYS.

When the results of key inventories and inspections reveal that there are lost keys or keys that cannot be accounted for, the key control custodian shall:

**a.** Report the lost or unaccounted for keys to the SSE, together with a list of the areas to which the keys provide access.

**b.** Determine in coordination with the SSE and the facility manager the extent to which locks shall be recored, changed, or otherwise modified to prevent compromise of existing safeguards.

**c.** Locksets, keys, and access control cards shall be stored in locked containers or secured storage areas.

**APPENDIX 10. SAFEGUARDING GOVERNMENT FUNDS****SECTION 1. STORAGE REQUIREMENTS****1. STORAGE OF FUNDS AVERAGING \$500 OR LESS.**

a. Funds shall be stored preferably in a GSA-approved security container, which has an internally affixed label stating the Federal specification that it was manufactured under and the security protection it affords and an external label reading "GENERAL SERVICES ADMINISTRATION-APPROVED SECURITY CONTAINER (MANUFACTURER'S NAME)".

b. As an alternative to "a" above, the funds may be stored in a metal file cabinet equipped with a steel bar and secured by a three position, dial type, changeable combination padlock approved for the purpose by the SSE.

**2. STORAGE OF FUNDS AVERAGING MORE THAN \$500 BUT LESS THAN \$2,000 ON HAND.**

a. Funds shall be stored in a GSA-approved security container.

b. During non-working hours, entry to the room, building, or structure in which the container is located shall be controlled by locking mechanisms approved by the SSE.

**3. STORAGE OF FUNDS AVERAGING MORE THAN \$2,000 BUT LESS THAN \$15,000 ON HAND.**

a. Funds shall be stored in a Class 1, 2, 4, or 5 GSA-approved security container.

b. As an alternative to "a" above, the funds may be stored in a mercantile safe which meets or exceeds Underwriters Laboratory requirements for a TL 30 label.

c. As an alternative to both "a" and "b" above, the funds may be stored in any GSA-approved security container, provided the specific room in which the container is located, or the container itself, is equipped with an approved alarm system, and the response to an activated alarm does not exceed 15 minutes.

**4. STORAGE OF FUNDS AVERAGING MORE THAN \$15,000 BUT LESS THAN \$50,000 ON HAND.**

a. Funds shall be stored in a Class 1, 2, 4, or 5 GSA-approved security container or in a mercantile safe which meets Underwriters Laboratory requirements for a TL 30 label.

b. The fund storage container shall be located in a fund storage room that meets the criteria specified in this order for fund storage rooms.

c. The container itself shall be equipped with an alarm system approved by the SSE.

**5. STORAGE OF FUNDS AVERAGING MORE THAN \$50,000 ON HAND.**

a. Funds shall be protected as specified in paragraph 4, above.

b. If practicable, the funds shall be divided into more than one approved container.

**6. COMBINATIONS TO FUND STORAGE CONTAINERS.**

Refer to FAA Order 2770.4.

7. **SUPPLEMENTAL SAFEGUARDS.** The SSE in evaluating the risk for a specific fund location may determine that supplemental safeguards, in addition to those required by FAA Order 2770.4, would be advisable to reduce vulnerability and risk. Supplemental safeguards could consist of one or more of the following:

- a. Panic or hold up alarm.
- b. CCTV monitored from a remote location.
- c. Hold up camera.
- d. Bullet resistant partitions.
- e. Money clip alarms.
- f. Daytime (during working hours) cleaning.
- g. Single entrance with provision for identifying individuals seeking admittance without opening the door.
- h. Hold up packets.

## SECTION 2. FUND STORAGE ROOMS

**8. REQUIREMENT.** When a Government fund averages \$15,000 or more on hand, the fund container shall be located in a fund storage room as an additional safeguard. Properly designed rooms, secured by high security lockset(s) approved by the SSE, can compensate for less desirable locations for the fund activity (e.g., located on the ground floor as opposed to an upper floor).

**9. FUND STORAGE ROOM DESIGN.** The basic design features that are required to be included in the construction specifications for a fund storage room are as follows:

**a. Walls, floors, and ceilings** shall be designed to minimize the possibility of forced or surreptitious entry. Planning shall provide for the use of an alarm system to overcome such construction deficiencies as insert-type wall panels and false ceilings (i.e., where the walls do not extend to ceiling deck). If an intrusion detection system (IDS) is considered, it is important to ensure that the IDS is approved by the SSE and the response time to an alarm is not more than 15 minutes.

**b. Doors.** The number of doors providing access to the fund storage room shall be kept to a minimum. Doors shall be constructed so as to afford reasonable resistance to forced entry. The following apply:

(1) Solid wood or metal doors shall be installed. If hollow doors are used, they shall be covered with 9 to 12-gauge security screen or 16-gauge sheet steel, fastened with security bolts or smooth head bolts, thoroughly bolted to the door. Nuts shall be peened to make unauthorized removal difficult.

(2) Hinges shall be heavy duty security type with non-removable pins.

**c. Window(s).** If possible, the fund storage room should not have any windows. Where this is not practical, the number of windows shall be kept to a minimum, and all windows shall be secured during non-duty hours. If the room has an exterior window or window on a hallway, it will be protected by steel security screens or steel bars as prescribed in this order or by an IDS approved for the purpose by the SSE.

**10. VENTS, CRAWLS SPACES, AND SUSPENDED CEILINGS.** These types of construction features should be examined by the SSE to determine if they will permit passage of a potential intruder. The following requirements apply:

**a. Openings for heating and ventilating ducts** shall be kept to a minimum. Duct terminals and connection points shall be in an exposed location, where they may be readily observed to detect tampering.

**b. Openings of 8 inches or larger** shall be protected with 9 to 12-gauge steel mesh. The steel mesh shall be either welded to the duct body or secured with round headed bolts, with nuts peened in place to make unauthorized removal difficult.

**11. PROTECTIVE LIGHTING.** Protective lighting requirements shall be identified by the SSE during the risk analysis of the fund storage room and procedures. In facilities where there is a security force that conducts patrols or where an area monitoring capability is provided such as CCTV, lighting should be provided for any fund container that is visible either from common hallways in the building or from outside the structure.

## APPENDIX 11. STANDARDS FOR THE SAFEGUARDING AND USE OF FIREARMS AND CHEMICAL IRRITANTS

### SECTION 1. INTRODUCTION

1. **PURPOSE.** The purpose is to establish the procedures to be followed to ensure that firearms are properly safeguarded, used, accounted for, and disposed of in accordance with this appendix.

#### 2. GENERAL REQUIREMENTS.

a. Personnel shall not be issued firearms or chemical irritants until they have been properly trained in their use and handling and are familiar with the provisions of this appendix.

b. This appendix shall be made a part of any contract entered into for private contract guard support for FAA facilities where the guards are required to carry firearms.

3. **USE OF FORCE.** Personnel duly authorized to possess or carry firearms in the performance of their duties, law enforcement or security activities, shall use only such force as is necessary to overcome any opposing force or threat by rendering the person(s) incapable of continuing the activity, which prompted the use of such force or weapon.

4. **DEADLY FORCE.** Deadly force is authorized only when the employee (or contractor-employee) has cause to believe that another person poses an imminent threat of death or serious bodily injury to the employee or others.

5. **TRAINING REQUIREMENT.** No FAA or contractor personnel shall be authorized to carry or use a firearm in performance of their FAA duties unless and until it is established in writing that he/she has been adequately trained and qualified and understands the DOT/FAA policies and standards.

6. **DRAWING A FIREARM.** A firearm shall be drawn only when it is intended to be employed in the protection of life.

7. **WARNING SHOTS.** Firing warning shots is prohibited.

8. **FLEEING PERSON.** Firing at a fleeing person is justified only when it is clearly in self defense or necessary to protect a person from death or serious bodily injury.

9. **FIRING FROM A MOVING VEHICLE.** Firing from a moving vehicle or at a fleeing motor vehicle is prohibited.

10. **POSSESSION OF PRIVATELY OWNED FIREARMS IN OR ON FAA-OWNED OR LEASED PROPERTY.** Except as provided for in paragraph 14 below, all persons while in or on FAA-owned or leased property, including vehicles, shall comply with the following:

a. No person shall carry or have in his/her possession firearms or other weapons unless authorized to do so in connection with his/her official duties.

b. FAA private contract security guard personnel shall not carry or have in their possession firearms or other weapons except those specifically authorized in the FAA contract.

11. **GENERAL SERVICES ADMINISTRATION (GSA) PROPERTY.** It is prohibited for any FAA employee to carry or have in his/her possession firearms or other weapons while on GSA-owned or leased property, including vehicles (Federal Property Management Regulation 41, CFR 101-20.312).

12. **EXCEPTION.** These prohibitions do not preclude FAA military or civilian personnel or their dependents who reside in Government-owned or leased housing from possessing firearms which are utilized for recreation or protection, providing such possession conforms to local law.

13. **CARRIAGE OF FIREARMS ABOARD COMMERCIAL AIRCRAFT.** Each FAA employee who is officially authorized to carry or transport a firearm or other dangerous weapon aboard a commercial aircraft shall fully comply with the applicable Federal Aviation Regulations (FAR).



## SECTION 2. CHEMICAL IRRITANTS

**14. DESCRIPTION.** Chemical irritants manufactured under various brand names, such as "mace," enable the user to exercise restraint over others. Different chemical compositions have varying degrees of hazard when improperly used. Manufacturers' instructions concerning use of the products must be understood and carefully followed.

### 15. RESTRICTIONS.

a. The chemical irritant shall be directed at a person at a minimum distance of 2 feet and only long enough to incapacitate the individual.

b. The chemical irritant must be aimed at the chest rather than at the face.

c. Chemical irritants shall not be used against a person who has an obvious incapacitation; has impaired breathing; or lacks normal protective reflexes.

d. A person who has been subdued with a chemical irritant must be permitted as soon as possible to wash with clear water and to use other antidotes as recommended by the manufacturer. If held in custody and adverse visual or respiratory effects continue, the individual shall be provided medical attention.

**16. CROWD CONTROL.** The above limitations do not apply in crowd control situations that require the use of chemical irritants as a last resort.

## SECTION 3. CONTRACT GUARD FORCE

**17. GENERAL.** Private contract guard personnel employed by the FAA are governed by the policies and procedures established in this appendix.

### 18. FAA CONTRACTING OFFICE

**REQUIREMENTS.** FAA logistics and contracting offices that initiate procurement requests for contract guard security services for FAA facilities shall:

a. Include in such procurement requests, a requirement that the provisions of this appendix be made a part of any resulting contract.

b. The manager of the facility or office requesting armed contract guard service shall coordinate all statements of work and requests for bid with the appropriate servicing security element prior to forwarding these documents to the contracting office.

c. The manager of the contracting office shall coordinate with the requesting office and the SSE as required to ensure that the wording and provisions of security guard contracts for armed guards services comply with the requirements of this appendix.

**19. GENERAL.** The manager of each FAA office or element which has procured Government-owned firearms and ammunition, or which intends to request such procurement, shall designate in writing a primary firearms custodian and one or more alternate firearms custodians as may be required.

### 20. PRIMARY AND ALTERNATE FIREARMS

**CUSTODIANS.** The primary firearms custodian, whenever possible, shall be selected from the office or element maintaining the firearm(s). The primary firearms custodian is authorized to designate the alternate firearms custodian(s) subject to the approval of the office or element manager.

**21. RECORDS AND NOTIFICATION.** Necessary procedures shall be established to ensure that the name, grade, job title, and duty assignment of each individual designated as primary and alternate custodian are provided in writing to the SSE and to the property officer of the servicing Logistics Division.

**22. DUTIES.** The custodian and, in his or her absence, the alternate custodian shall:

a. Obtain approval for and initiate procurement requests for firearms and ammunition.

b. Receipt for and accept custody of firearms and ammunition.

c. Establish procedures for accountability, issuance, control, and safeguarding of firearms and ammunition in his or her custody, which include the conduct of periodic inventories, and supervision of the issuance and turn in of weapons and ammunition.

d. Ensure compliance with the requirements of this appendix concerning issuance, physical security, and storage of firearms and ammunition.

e. Promptly report lost or stolen firearms and ammunition to the SSE. Reference: (FAA Order 4650.21B).

f. Report promptly to the SSE any known or suspected instances of improper safeguarding, handling, or use of firearms and ammunition.

g. Establish safeguarding procedures to provide for secure shipment of firearms and ammunition designated for disposal, transfer, or other purposes in accordance with FAA policy.

h. Maintain appropriate records.

**23. ISSUANCE AND ACCOUNTABILITY.** FAA employees shall be issued a Government-owned firearm only when their officially assigned duties fall into categories specifically approved by the Administrator that require the employee to be armed. These categories include those listed in the following paragraphs.

**24. FEDERAL AIR MARSHALS.** This category includes Federal Air Marshals and such other FAA personnel who may be assigned law enforcement duties by the Administrator which specifically require the individual to be armed.

**25. SURVIVAL AND EMERGENCY FIREARMS.** FAA employees who are making an official flight or traveling in an operational area, such as Alaska, where Federal, state, or local authority requires that a firearm be part of the emergency survival equipment.

**26. ISSUANCE OF SURVIVAL KITS.** Issuance of a survival kit containing a firearm in a metal container with unbroken seal, which is carried on board an aircraft to meet the requirement identified in paragraph 24, is not considered as constructive issuance of a firearm so long as the seal is intact and the kit has not been opened.

**27. ISSUANCE TO CONTRACT GUARD PERSONNEL.** Issuance of Government-owned firearms to private contract guard personnel is prohibited.

**28. CUSTODIAN.** A custodian or alternate custodian shall not issue a firearm to an individual until the custodian has verified that the individual meets all of the criteria listed in this section.

**29. AUTHORITY.** The individual must be authorized by the Administrator to carry a firearm in the performance of his/her official duties with FAA.

**30. TRAINING.** The individual must as a minimum have written certification that he or she has successfully completed the firearms training specified in this appendix. Certification shall include the number of hours of training, whether the training was classroom or on-the-job, and a score or indication of successful completion of instruction by the individual.

**31. QUALIFICATION.** The individual must have successfully qualified within the past 12 months with the type of weapon to be issued. Qualification must have been accomplished on a recognized law enforcement or other approved range under the supervision of a certified firearms instructor and using approved qualification firing exercises.

**32. KNOWLEDGE OF POLICY AND REGULATIONS.** The individual must certify in writing that he or she has read and understands FAA firearms policies, standards, and procedures for safeguarding firearms as specified in this appendix.

**33. KNOWLEDGE OF FIREARMS CARE.** The individual must demonstrate to the satisfaction of the firearms instructor that he or she understands the proper procedures for the care and cleaning of the firearm.

**34. ISSUANCE OF SURVIVAL KIT FIREARMS.** In the case of survival firearms, training is desirable; however, knowledge of the contents of this appendix is mandatory.

**35. GENERAL.** Firearms shall be receipted for under the supervision of the appropriate firearms custodian who will ensure that either signed receipt, exchange card system, or comparable control system is established and maintained.

**36. RECEIPTS.** Receipts shall contain the following information:

a. Name and "ID" card number of the individual receiving the firearm.

b. Name of the issuing official (firearms custodian).

c. Office and duty assignment of the individual receiving the firearm.

d. Date of issuance and place of issue.

e. Identifying data for the firearms (serial number, manufacturer, etc.).

f. Purpose for which the firearm is issued (e.g., law enforcement duties).

## SECTION 5. INVENTORY REQUIREMENTS

**37. ANNUAL INVENTORY.** The firearms custodian shall have an annual inventory by serial number of all firearms charged to his/her custody conducted by disinterested representatives of Logistics or Property Management Branch on or before June 30 of each calendar year.

**38. UNSCHEDULED INVENTORIES.** Irregular inventories of firearms and ammunition shall be conducted as required by appropriate Property Management and Logistics directives and may be conducted at any time by the firearms custodian.

**39. SPOT CHECK AND SPECIAL INVENTORIES.** Spot checks and special inventories of firearms and ammunition shall be conducted as required by Property Management or Logistics directives, at the discretion of the firearms custodian or when so directed by the SSE.

**40. CHANGE OF CUSTODIAN.** Whenever there is a change of firearms custodian, a joint inventory shall be conducted of all Government-owned firearms by the old and new custodian, prior to the new custodian receipting for the firearms.

**41. INVENTORY REPORTS.** Inventory reports in writing shall be prepared by the firearms custodian at the completion of each required inventory. Format for the reports shall follow the guidelines set forth in FAA Order 4633, Physical Inventory.

### **42. DISTRIBUTION OF INVENTORY REPORTS.**

Inventory reports shall be distributed as follows:

a. Firearms custodian—one copy of current inventory for file.

b. Servicing security element—one copy of current inventory.

c. Additional copies shall be provided to the appropriate Logistics or Property Management Office as required to comply with applicable FAA directives for the element concerned.

**43. INVENTORY DISCREPANCIES.** Inventory discrepancies shall be reported by the firearms custodian immediately to the SSE and to the appropriate Logistics or Property Management Office.

## SECTION 6. PHYSICAL SECURITY SAFEGUARDS

**44. REQUIREMENTS.** Firearms shall be stored in GSA-approved security containers at all times when not in official use.

### **45. PHYSICAL SECURITY.**

a. Firearms shall be stored only in areas that have been approved by the SSE.

b. Under no circumstances will firearms and ammunition be stored in the same security container.

c. The room in which the firearms storage container is to be located shall be of overall substantial construction.

d. The walls of the room shall extend from true floor to true ceiling if the area is not 24-hour operational.

e. The room shall, if possible, have no windows or other openings and shall meet strongroom requirements.

f. The room shall have only one entrance door of solid wood or metal construction a minimum of 1-3/4 inches thick installed using heavy-duty builders hardware throughout.

g. The door shall be hung in such a manner that the hinges are either concealed or the hinge pins are peened or spot welded to deter unauthorized removal.

h. All doors shall be secured by a high-security key actuated padlock (FSN 5340-799-8248) and associated hasp (FSN K2 5340-178-7875).

**46. INTRUSION DETECTION SYSTEM (IDS).** Each facility with a firearms storage room shall be provided with an intrusion detection system approved for that purpose by the SSE.

**47. PROTECTIVE LIGHTING.** External illumination shall be provided over all entrances to the arms storage room or building. If the storage room has windows, lighting shall also be maintained within the storage room or building during hours of darkness to facilitate security checks.

**48. SECURITY FORCE PATROLS.** All arms and ammunition storage rooms or buildings shall be periodically checked by guards.

**49. SEPARATE STORAGE OF KEY FIREARMS PARTS.** Where feasible, sliding bolts or other vital parts which render small arms inoperable when removed shall be stored separately.

**50. STORAGE.** Ten handguns or less shall be stored in a GSA-approved security container of the type approved for the storage of classified information.

**51. GUN LOCKER STORAGE.** With the approval of the servicing security element, handguns in quantities of 10 may be stored in standard gun lockers of the type approved for use by law enforcement agencies.

**52. STORAGE IN QUANTITIES GREATER THAN 10.** Handguns in numbers greater than 10 shall be stored in a GSA-approved, Class-5, U.S. Government Security Weapons Storage Container, equipped with a built-in, Group 1R, three position, dial-type, changeable combination lock (Reference Federal Specification AAF-36313, GSA-FAA).

**53. UNAVAILABILITY OF CLASS 5 CONTAINER.**

When a container, such as that noted in paragraph 51 above, is not available, the following alternative safeguards shall be employed:

a. Handguns shall be stored in a GSA-approved container of the a type approved for the storage of classified security information.

b. The container shall be located in a physically secure room which has been approved for this specific purpose by the servicing security element.

**54. STORAGE OF RIFLES, CARBINES, AND SHOTGUNS.** Rifles, carbines, and shotguns shall be stored in a GSA-approved, Class-5 U.S. Government Weapons Storage Container, equipped with a built-in, Group 1R, three position, dial-type, changeable combination lock.

**55. EXCEPTIONS TO STORAGE REQUIREMENTS.** Requests for exceptions to this standard must be submitted in writing with appropriate justification through the servicing security element to ACP-120.

**56. STORAGE.** Ammunition shall be stored in a GSA-approved security container

**57. STORAGE.** Survival kits containing firearms shall, as a minimum, be stored in a room of substantial construction which has been approved for that purpose by the servicing security element.

**58. RESPONSIBILITY FOR FIREARMS CONTAINER.** The firearms custodian is responsible for control of the firearms storage container.

**59. STORAGE CONTAINER COMBINATION.** Combinations to firearms storage containers shall be strictly controlled and safeguarded.

a. Combinations shall be changed at least once during each 12-month period.

b. Combinations shall be changed at any time that a person having knowledge of the combination is reassigned or no longer authorized access to the container.

c. Combinations will be changed when there is reason to believe that the combination has been compromised.

**60. SECURITY CONTAINER CHECK SHEET.** A Security Container Check Sheet (SF 702) (NSN: 7540-01-213-7899) shall be affixed to each container and shall be filled in whenever the container is opened or locked.

**61. OPEN/CLOSED SIGNS.** Reversible cardboard CLOSED-OPEN signs (GSA Supply No. 9905-286-7021 or equivalent) shall be used as additional reminders on firearms storage containers.

**62. LOCKING REQUIREMENT.** The firearms storage container shall be locked at all times when not in actual use.

## SECTION 7. LOSS OR THEFT OF GOVERNMENT-OWNED FIREARMS

**63. REPORTING REQUIREMENTS.** The individual who becomes aware of the loss or theft of a firearm shall:

a. Notify the local police.

b. Notify the firearms custodian and advise him/her of the circumstances surrounding the loss or theft.

c. Notify the servicing security element if unable to reach the firearms custodian.

d. Within 24-hours from the time the loss or theft is discovered, prepare a complete written report for submission through the firearms custodian to the servicing security element.

**64. FIREARM LOSS OR THEFT REPORT CONTENT.** The report of loss/theft submitted by the individual shall be typewritten in memorandum format and shall, as a minimum, contain the following information. (See also requirements of FAA Order 4650.21B).

a. Complete identifying data concerning the firearm.

b. Location where the loss or theft occurred and details of safeguards taken to protect the firearm.

c. Date and approximate time when the loss or theft occurred.

d. Time when the loss or theft was first discovered.

e. Purpose for which the firearm was originally issued.

f. Names of all persons who were with the responsible individual at the time of the loss or theft or who could provide additional information.

g. A narrative description of how the firearm was lost and/or the circumstances surrounding the theft.

h. Actions taken by the individual upon discovery of loss or theft, including notification of proper local police, etc.

**65. ACTION BY THE FIREARMS CUSTODIAN.** Upon receipt of a report of loss or theft of a Government-owned firearm, the firearms custodian shall:

a. Promptly inform the servicing security element of the loss or theft and provide complete information concerning the identifying data on the firearm.

b. Prepare a Report of Survey in accordance with FAA Order 4630.3.

**66. ACTION BY THE SERVICING SECURITY ELEMENT.** The servicing security element upon receipt of notification that a Government-owned firearm has been lost or stolen shall:

a. Ensure that complete information concerning the lost or stolen firearm(s) has been supplied to the appropriate police jurisdiction and to the FBI.

b. Notify ACO-1 by the most expeditious means available of the loss or theft.

c. Initiate appropriate investigative activity and follow-up. Assign responsibility for the loss whenever possible, and determine what administrative or disciplinary action should be taken.

d. The servicing security element's manager shall forward the results of the investigation to ACO-1. The managers' disciplinary action plan must be attached to the report.

## SECTION 8. FIREARMS TRAINING

**67. APPROVED FIREARMS TRAINING PROGRAMS.** Any formal firearms training program conducted by a Federal, state, or local law enforcement agency and approved for the training and qualification of law enforcement officers.

**68. SPECIAL TRAINING PROGRAMS.** Specialized training developed by ACZ-1 for the training of Federal Air Marshals.

**69. QUALIFICATION STANDARDS.** FAA law enforcement and security personnel shall successfully complete an approved law enforcement firearms training program or special firearms training program which includes attainment of the minimum score established for range qualification.

**70. FAILURE TO COMPLETE REQUIRED TRAINING SUCCESSFULLY.** Individuals failing to complete successfully an approved firearms training program shall not be issued a Government-owned firearm or authorized to carry a firearm in the conduct of their official duties until they have successfully completed all training and qualification requirements.

**71. TRAINING AND QUALIFICATION RECORDS.** Firearms training and qualification records for FAA law enforcement and security personnel shall be maintained current and reflect all pertinent data regarding formal firearms training received, instruction in FAA firearms policy, and range scores for each individual authorized to carry a firearm.

**72. INSPECTION OF FIREARMS TRAINING RECORDS.** Training and qualification records are subject to "spot checks" and inspections by the servicing security element and by the firearms custodian and will be included as an integral part of regularly scheduled inspections and surveys conducted by the servicing security element.

## SECTION 9. FIREARMS TRAINING FOR CONTRACT GUARDS

**73. TRAINING CERTIFICATION.** Contractors employed by the FAA to provide armed security guard service shall not be authorized to issue a firearm to their employees until the contractor has certified in writing to the FAA contracting officer's technical representative (COTR) that the individual has successfully completed a federally-approved firearms training program. The certification shall:

a. Include certification of the fact that the employee has qualified within the preceding 12-month period in the use of the firearm to be issued.

b. Include the statement that the contractor and the employee have complied fully with all requirements of this appendix that pertain to private contract guard personnel.

**74. CONTRACT REQUIREMENT.** This appendix shall be an integral part of any contract issued by an FAA contracting officer or office for armed private contract security services at FAA facilities.

a. A copy of the contract for armed security guard services, together with all certification responses from the guard service contractor, shall be furnished by the contracting officer to the servicing security element.

b. Current copies of the training and qualification records for contract guard personnel shall be provided by the guard contractor to the FAA COTR at each facility. The COTR will retain these records and make them available upon request to the servicing security element.

## SECTION 10. REQUALIFICATION

**75. REQUIREMENT.** Individuals who have successfully completed an approved firearms training program shall be required to requalify with their firearm as a minimum on an annual basis.

**76. REQUALIFICATION OF PRIVATE CONTRACT GUARD PERSONNEL.** Where FAA has contracted for armed private contract guard services, the contract shall include the requirement for requalification on an annual basis or more frequently if considered necessary for each guard employee authorized to carry a firearm.

### **77. ACTIONS TO BE TAKEN UPON FAILURE OF CONTRACT GUARD EMPLOYEE TO REQUALIFY.**

Contract requirements for armed private contract guards shall stipulate that failure of a contract security guard employee to requalify with his/her firearm will constitute basis for immediate suspension of authorization for that individual to carry a firearm on FAA property. This suspension shall last until such time as the employee successfully qualifies.

**78. ACTIONS TO BE TAKEN FOR FAA EMPLOYEES WHO FAIL TO REQUALIFY.** Law enforcement and security personnel for the FAA who fail to requalify shall be reexamined immediately. Failure to requalify shall constitute basis for immediate suspension of authorization of individual to carry a firearm.

**79. TRAINING FOR FAA EMPLOYEES ISSUED SURVIVAL KITS.** FAA personnel are not required to have successfully completed an approved firearms training and qualification program to be issued survival kits containing firearms. Familiarization firing with the type of firearm contained in the survival kit is desirable and should be accomplished whenever possible.

## SECTION 11. FIREARMS INCIDENTS

### **80. REPORTING OF FIREARMS INCIDENTS.**

All incidents involving the discharge of a firearm by an FAA employee or by a private contract security guard employed by the FAA will be reported in accordance with this section and other applicable FAA directives.

**81. INDIVIDUAL RESPONSIBILITY.** Each FAA employee and private contract security guard employee authorized to carry a firearm on FAA property is fully liable and responsible for actions taken involving the use of the

firearm. FAA employees are specifically prohibited from using firearms in the performance of their duties except as authorized by this appendix.

**82. INCIDENT REPORTING.** A written report shall be rendered to the SSE any time that a firearm is accidentally discharged for any reason. This reporting requirement is mandatory, regardless of whether or not personal injury resulted from the discharge.

**83. PROCEDURES TO BE FOLLOWED BY THE INDIVIDUAL.** The individual responsible for the discharge of the firearm shall immediately notify his/her supervisor of the incident and the circumstances relating thereto.

a. The report shall include any injury or fatality which may have resulted from the use of the firearm, including injuries resulting from accidental discharges.

b. In the event that the individual responsible is not able to initiate reporting action, it shall be the responsibility of his/her supervisor to make the report.

**84. ACTIONS TO BE TAKEN BY THE SUPERVISOR.** The supervisor upon notification that a firearm has been discharged, shall take the following actions:

a. Ensure that action has been taken to notify the appropriate authorities if a fatality, injury, or damage to private property occurs,

b. Request medical aid if needed.

c. Notify the servicing security element by the most expeditious means available, and provide a written follow-up report of the incident within 24-hours.

**85. INCIDENT REPORT.** The written incident report submitted by the supervisor shall contain as a minimum the following information:

a. Name and duty assignment of the individual having custody of the firearm.

b. Time of the firearm discharge (date/day/hour).

c. Reason for firing the weapon.

d. Activity in which the individual was engaged when the weapon was fired.

e. Injury, fatalities, or property damage resulting from the discharge.

f. Names of any witnesses having knowledge of the incident.

**86. ACTIONS TO BE TAKEN BY THE SERVICING SECURITY ELEMENT.** The FAA servicing security element upon notification of a firearm incident shall:

a. Notify ACO-1 of the incident and the circumstances. Notification shall include any injuries or fatalities and those agencies/authorities notified of the incident.

b. Notify the Regional Administrator or center or service director of the incident and the circumstances.

c. Obtain as soon as possible a written report containing full details on the discharge of the firearm. Conduct an investigation of the incident.

## APPENDIX 12. STORAGE CONTAINERS, VAULTS, AND STRONGROOMS

### SECTION 1. SECURITY CONTAINERS

**1. SECURITY CONTAINERS.** Security containers are containers that have been specifically developed by the manufacturer and approved by GSA for the storage of classified material.

**2. CLASSES OF SECURITY CONTAINERS.**

Specifications have been developed for 7 classes of security containers; however, only Classes 1, 5, and 6 are now available on the Federal Supply Schedule. Prior to selection of a particular security container, FAA managers shall coordinate with the SSE to ensure that the container selected will be adequate for their needs.

**3. CLASS 1 CONTAINER.** The Class 1 security container is insulated and comes in several models which include both a 2-drawer and 4-drawer version. Provision can be made to have more than one locking drawer to meet compartmentation requirements. The physical security protection provided by the Class 1 is expressed on the test certification label as:

- a. 30 man-minutes against surreptitious entry.
- b. 10 man-minutes against forced entry.
- c. 20 man-hours against lock manipulation.
- d. 20 man-hours against radiological attack.
- e. 1 man-hour against fire damage to contents.

**4. CLASS 5 CONTAINER.** The Class 5 security container offers the maximum physical security protection expressed on the test certification label as follows:

- a. 30 man-minutes against surreptitious entry.
- b. 10 man-minutes against forced entry.
- c. 20 man-hours against manipulation of the lock.
- d. 20 man-hours against radiological attack.

**5. CLASS 6 CONTAINER.** The Class 6 security container affords the same protection as the Class 5 except there is **no forced entry protection**. It is available in 2-, 4-, and 5-drawer models and in a map and plan cabinet. The physical security protection provided is expressed on the test certification label as:

- a. 30 man-minutes against surreptitious entry.
- b. 20 man-minutes against manipulation of the lock.
- c. 20 man-hours against radiological attack.
- d. No forced entry requirement.

### SECTION 2. VAULTS

**6. CLASS A VAULT.**

a. Floor and walls shall be constructed of 8-inch thick reinforced concrete. Walls shall extend to the underside of the roof slab above.

b. Roof shall be constructed of monolithic concrete slab of a thickness to be determined by structural requirements, but not less thick than the walls and roof.

c. Ceiling. Where the roof construction is not in accordance with subparagraph "b" above, a normal reinforced concrete slab will be placed over the vault area at a height not to exceed 9 feet.

d. Vault door and frame unit shall conform to the Federal Specification for Class 5 vault doors.

**7. CLASS B VAULT.**

a. Floor shall be of monolithic concrete construction of the thickness of adjacent concrete floor construction, but not less than 4 inches (10 centimeters) thick.

b. Walls shall be of not less than 8 inch (20 centimeters) thick brick, concrete block, or other masonry units. Hollow masonry units shall be the vertical cell type (load bearing) filled with concrete and steel reinforcement bars. Monolithic steel-reinforced concrete walls at least 4 inches (10 centimeters) thick may be used and are required in seismic areas.

c. Roof construction shall be of monolithic reinforced concrete slab of a thickness to be determined by structural requirements, but not less than 4 inches (10 centimeters) thick.



d. **Ceiling.** Where the roof construction is not in accordance with paragraph "c" above, a normal reinforced concrete slab shall be placed over the vault at a height not to exceed 9 feet (2.7 meters).

#### 8. CLASS C VAULT.

a. **Floor** construction requirements shall be the same as for a Class B vault.

b. **Walls** shall be constructed of not less than 8 inch (20 centimeter) thick hollow clay tile vertical cell (double shell) or concrete block (thick shell). Monolithic steel-reinforced concrete walls at least 4 inches (10 centimeters) thick may also be used and shall be used in seismic areas. Walls back of the exterior wall of the building shall be concrete solid masonry, or hollow masonry filled with concrete and steel reinforcing bars.

c. **Roof** construction shall be the same as that required for a Class B vault.

d. **Ceiling** construction shall be the same as that required for a Class B vault.

e. **Vault door and frame unit** shall conform to Federal specifications for Class 6 vault doors.

### SECTION 3. STRONGROOMS

9. **DESCRIPTION.** Strongrooms should be considered as an interior space enclosed by, or separated from, other similar spaces within an FAA facility by four walls, a ceiling, and a floor, all of which are normally constructed of solid building materials.

a. Under this criteria, rooms having false ceilings and walls constructed of fabrics or other similar material shall not qualify as strongrooms.

b. Facility managers shall coordinate with the SSE when considering the construction of strongrooms to evaluate the need and consider alternatives.

#### 10. CONSTRUCTION REQUIREMENTS.

a. **Hardware.** Heavy-duty builder's hardware shall be used in construction of strongrooms. All screws, nuts, bolts, hasps, clamps, bars, hinges, pins, etc., shall be securely fastened to preclude surreptitious entry and ensure visual evidence of forced entry. Hardware accessible from outside the area shall be peened, brazed, or otherwise modified in a manner approved by the SSE to make unauthorized removal difficult.

b. **Walls and ceiling** construction shall be of plaster, gypsum board, metal, hardboard, wood, plywood, Number 9-gauge, 2-inch wire mesh or stronger, or other material offering similar resistance to, or evidence of, unauthorized entry into the area. **Insert type panels** shall not be used.

c. **Floor** shall be of solid construction, utilizing materials like concrete, ceramic tile, wood, etc.

d. **Window** openings shall be fitted with 0.5 inch (1.25 centimeter) steel bars, separated by not more than 6 inches (15 centimeters) on center, with cross bars to prevent

spreading spaced not more than 12 inches (30 centimeters) apart, or, Number 9-gauge security mesh fastened by bolts extending through the wall and secured on the interior side of the window frame. **In addition to being kept closed at all times, the windows shall also be opaqued by any practical method, such as paint on both sides of the window, or covering the entire window opening on the interior side with tempered masonite, sheet metal, plywood, etc.**

e. **Miscellaneous openings.** Where ducts, registers, sewers, and tunnels have an area of 96 square inches (0.06 meters) or more and constitute possible points of unauthorized access, they shall be equipped with man-barriers such as Number 9-gauge wire mesh, with 2-inch (5 centimeter) square mesh or steel bars of at least 0.5 inch (1.25 centimeter) in diameter extending across their width with a maximum spacing between bars of not more than 6 inches (15 centimeters) on center. The steel bars shall be securely fastened at both ends to preclude removal with cross bars to prevent spreading.

f. **Doors** may be of metal construction or of solid wood construction reinforced with a metal plate on the interior side. When doors are used in pairs, an astragal (overlapping molding) shall be used where the doors meet. When the construction is of Number 9-gauge, 2-inch (5 centimeter) wire mesh, a door constructed of similar material may also be used. However, the wire mesh door shall be reinforced with a metal panel at least 36 inches (90 centimeters) wide from floor to ceiling welded to the inside of the wire mesh wall next to the locking device.

**g. Door louvers and baffles plates** should be avoided wherever possible. Where these features are used, they shall be reinforced with Number 9-gauge wire mesh, with 2-inch square mesh fastened to the inside of the door and covering the louvers or baffles.

**h. Door locking devices.** Doors shall be secured by a built-in three position, Group 1R, dial-type changeable combination lock with deadbolt extension, and reinforced strike. If the strongroom construction is of Number 9-gauge, 2-inch (5 centimeter) security mesh, the locking devices shall be alarmed to detect tampering with the lock. Locking devices and alarm systems (where applicable) must be of a type approved by the SSE and the installation must be inspected by the SSE before the alarm is placed into operation.

## **11. STORAGE OF CLASSIFIED INFORMATION.**

Vaults and strongrooms shall not be used for open storage of classified material, as a substitute for the security container requirements specified in FAA Order 1600.2, for the safeguarding of national security classified information, and material, without the written approval of the SSE.

**12. COMBINATIONS FOR VAULTS AND STRONGROOMS.** Combinations for vaults and strongrooms shall be recorded, controlled, changed, and accounted for in accordance with the requirements for safeguarding and controlling combinations contained in FAA Order 1600.2.

## APPENDIX 13. TYPES OF FAA FACILITIES

The facilities listed are typical examples of FAA administrative and operational facilities that would fall under the provisions of the PSMP.

AERONAUTICAL CENTER—MIKE MONRONEY  
AIRCRAFT CERTIFICATION OFFICE—ACO  
AIR CARRIER DISTRICT OFFICES—ACDO  
AIR ROUTE SURVEILLANCE RADAR—ARSR  
AREA CONTROL FACILITY—ACF  
AIRCRAFT MAINTENANCE BASE—AMB  
AIRPORTS DISTRICT OFFICE—ADO  
AIRPORT TRAFFIC CONTROL TOWER—ATCT  
AIR ROUTE TRAFFIC CONTROL CENTER—ARTCC  
AIR TRAFFIC REPRESENTATIVES—ATREP  
AIRWAY FACILITIES SECTOR—AFS  
AIRWAY FACILITIES SECTOR FIELD OFFICE—AFSFO  
AIRWAY FACILITIES SECTOR FIELD OFFICE UNIT—AFSFOU  
AIRWAY FACILITIES SECTOR FIELD UNIT—AFSFU  
AUTOMATED FLIGHT SERVICE STATION—AFSS  
CENTER RADAR APPROACH CONTROL—CERAP  
CIVIL AVIATION SECURITY FIELD OFFICES—CASFO  
COMBINED APPROACH CONTROL/INTERNATIONAL STATION—CAPIS  
EMERGENCY OPERATIONS FACILITY—EOF  
FLIGHT INSPECTION FIELD OFFICES—FIFO  
FLIGHT SERVICE STATION—FSS  
FLIGHT STANDARDS DISTRICT OFFICE—FSDO  
GENERAL AVIATION DISTRICT OFFICE—GADO  
INTERNATIONAL AERONAUTICAL TELECOMMUNICATIONS SWITCHING CENTER—IATSC  
INTERNATIONAL FIELD OFFICE—IFO  
INTERNATIONAL FLIGHT SERVICE STATION—IFSS  
JOINT SURVEILLANCE SITES—JSS  
LOCAL CONTROL FACILITIES—LCF

MANUFACTURING INSPECTION DISTRICT OFFICE—MIDO  
METRO CONTROL FACILITY—MCF  
NATIONAL COMMUNICATIONS CENTER—NATCOM  
NATIONAL DATA INTERCHANGE NETWORK—NADIN  
RADAR AIR TRAFFIC CONTROL FACILITY—RATCF  
RADAR APPROACH CONTROL FACILITY—RAPCON  
REGIONAL HEADQUARTERS—RO  
SATELLITE EARTH STATION—SAT  
TERMINAL RADAR APPROACH CONTROL—TRACON  
TECHNICAL CENTER—FEDERAL AVIATION

**APPENDIX 14. FACILITY PHYSICAL SECURITY MANAGEMENT PLAN****CLASSIFICATION**

DATE:

FACILITY:

ADDRESS:

CITY:

STATE:

ZIP:

LOCATION ID:

FACILITY TYPE:

CATEGORY:

FACILITY MANAGER:

FACILITY SECURITY MANAGEMENT PLAN COORDINATOR:

**FACILITY SECURITY MANAGEMENT PLAN****1. Purpose.**

State purpose of plan.

**2. Area Security.**

Define the areas, buildings, and other structures considered critical and establish priorities for their protection.

**3. Integrated Security Management System.** Refers to the coordinated combination of equipment, personnel, and procedures used to neutralize security vulnerability. Integrated security measures to be considered in developing the facility security management plan include the areas listed in the following paragraphs.

**4. Control Measures.** Define and establish restrictions on access and movement into critical areas. These restrictions can be categorized as to personnel, vehicles, and materials.

**a. Personnel Access**

**(1) Establish controls pertinent to each area or structure.**

**(a) Authority for access.**

**(b) Access criteria for:**

1. Assigned personnel.
2. Visitors.

3. Maintenance personnel.

4. Contractor personnel.

**(2) Identification and control.**

**(a) Describe the system to be used in each area.** If a badge system is used, a complete description covering all aspects will be used in disseminating requirements for identification and control of personnel conducting business on the facility.

**(b) Application of the system.**

1. Assigned personnel.
2. Visitors to restricted areas.
3. Visitors to non-restricted areas.
4. Vendors, tradesmen etc.
5. Contractor personnel.
6. Maintenance and support personnel.

**b. Material Control**

**(1) Incoming.**

(a) Requirements for admission of material and supplies.

(b) Search and inspection of material for possible criminal/sabotage/terrorist hazards.

(c) Special controls on delivery of supplies and/or personnel shipments in restricted areas.

**(2) Outgoing.**

(a) Documentation required.

(b) Controls, as outlined in (1)(a), (b), and (c) above.

(c) Classified shipments not involving hazardous materials.

**(3) Hazardous materials.**

(a) Controls on movement of hazardous material on the facility.

(b) Controls on shipments or movement of hazardous material outside the facility.

**c. Vehicle Control.**

(1) Policy on administrative inspection of Government and privately owned vehicles.

(2) Parking regulations.

(3) Controls for entrance into restricted and nonrestricted areas.

(a) Privately owned vehicles.

(b) Facility vehicles.

(c) Emergency vehicles.

**d. Vehicle Registration.**

**5. Aids to Security.**

Indicate the manner in which the following listed aids to security are to be implemented on the facility.

**a. Protective barriers.**

(1) Definition.

(2) Clear zones.

(a) Criteria.

(b) Maintenance.

(3) Signs.

(a) Types.

(b) Posting.

(4) Gates.

(a) Types.

(b) Posting.

(c) Lock security/key control.

**b. Protective Lighting Systems.**

(1) Types.

(2) Use and control.

(3) Inspection.

(4) Action to be taken in the event of commercial power failure.

(5) Action to be taken in the event of a failure of alternate source of power.

(6) Emergency lighting systems.

(a) Stationary.

(b) Portable.

**c. Closed Circuit Television (CCTV).**

(1) Type and location of equipment.

(2) IDS verification capabilities.

(3) Sensitive area coverage.

(4) Recording procedures.

(5) Special system capabilities.

**d. Intrusion Detection Systems.**

(1) Security classification.

(2) Types.

(3) Type and area to be used.

(4) Inspection.

(5) Use and monitoring.

(6) Action to be taken in event of "Alarm" conditions.

(7) Maintenance.

(8) Alarm logs or registers.

(9) Sensitivity settings.

(10) Type of line supervision and tamper-proof provisions.

(11) Monitor panel location.

**e. Communications.**

(1) Types.

(2) Locations.

- (3) Use.
- (4) Tests.
- (5) Authentication.

#### 6. Guard Personnel.

Include general instructions that apply to all guard personnel (fixed and mobile). Detailed instructions such as Special Orders and SOP will be highlighted.

- a. Contract/Non-contract.
- b. Composition and organization.
- c. Tour of duty.
- d. Essential posts and routes.
- e. Weapons and equipment.
- f. Training.
- g. Methods of apprehension.
- h. Crisis response force.
  - (1) Composition.
  - (2) Mission.
  - (3) Weapons and equipment.
  - (4) Location.
  - (5) Deployment concept.

#### 7. Threat Levels/Crisis Management.

Indicate required actions in response to various emergency situations.

#### 8. Coordinating Instructions.

Indicate matters which require coordination with military or non-Government agencies.

a. Integration with plans host, tenant, or nearby military installations.

b. Liaison and coordination.

- (1) Local civil authorities.
- (2) Federal agencies.
- (3) Military organizations.

/s/ \_\_\_\_\_

#### Enclosures:

A—Threat assessment.

B—Facility Security Status Map (including explanation of Federal, state, and local jurisdictional responsibilities that have an impact on the security plan).

## APPENDIX 15. SECURITY SURVEY PROCEDURES

### SECTION 1. INTRODUCTION

**1. PURPOSE.** The procedures covered in this appendix identify considerations and principles which must be taken into account if a survey is to be successful. The techniques covered are well established security procedures that will help the individual agent and/or the survey team increase his/her/its effectiveness and efficiency and improve interrelationships with the facility being surveyed.

### SECTION 2. PERSONAL CONSIDERATIONS

#### 2. HELPFULNESS.

a. One of the primary benefits of the FAA Physical Security Survey and Inspection Program (PSSIP) is to take an objective look at the FAA facility. It should be realized that a survey team member's experience level shall recognize good security practices, and the ability to identify deficiencies in the facility's Physical Security Resource Management Program.

b. It is the job of the survey team member to pay attention to those things that are important (i.e., chronic, persistent, or trends). A "so what" test should be given to each deficiency and there should be an identifiable effect or impact. This is especially important for performance discrepancies not governed by requirements specified in FAA orders or directives.

c. On-the-spot corrections of minor discrepancies, the image of the individual inspector or the inspecting team will be enhanced as a cooperative and interested party by identifying the deficiencies which shall not be included in the final report.



**APPENDIX 16. ACCREDITATION EVALUATION CERTIFICATION**

The accreditation letter is a formal notification by the Manager of the Servicing Security Element (SSE) to the Facility Manager stating that the evaluated facility meets basic physical security standards established by the Physical Security Management Program and that the facility manager agrees to abide by the requirements of FAA Order 1600.6C. Once executed, the accreditation letter shall remain in effect until significant changes occur directly impacting physical security of the asset or major new construction projects or reconfiguration of the accredited facility takes place. A facility that meets accreditation requirements shall be issued an accreditation letter signed by the manager of the supporting SSE within 45 calendar days of an accreditation evaluation.

Facility accreditation notification shall:

- a. Be a formal letter addressed to the facility manager executed by the accrediting SSE manager.
- b. Include the name and address of the accredited facility.
- c. Specify the effective date of accreditation.

d. Identify the type of facility accredited-air route traffic control center (ARTCC), area control center (ACO), test center, etc.

e. Identify by name and title, the facility manager present during the accreditation evaluation.

f. Include a general physical description of the facility and security protective measures in place at the time of accreditation.

g. Comment on the criticality of the facility.

h. Identify the name and title of accreditation inspectors who actually conducted the evaluation.

i. Certifications shall also include the following declarative statement: This accreditation is granted based on the physical security management practices and procedures in effect at the time of the evaluation. Significant changes in physical security management procedures, internal or external facility configuration, or to its associated environment may require a reevaluation by the SSE.

## APPENDIX 17. FACILITY INSPECTION REPORTING SUBSYSTEM (FIRS)

### SECTION 1. INTRODUCTION

**1. PURPOSE.** The procedures and responsibilities covered in this appendix establish the Civil Aviation Security Information System's (CASIS) Facility Inspection Reporting Subsystem (FIRS) as the process and reporting format to be used exclusively by all elements of Civil Aviation Security (CAS) to report data obtained as a result of physical security inspections of FAA facilities and operations agencywide.

**2. AUTHORITY.** Standards covered in this appendix are based on this order, regulations, and directives listed in Appendix 1.

**3. EFFECTIVE DATE.** Implementation of FIRS agencywide began on November 1, 1990, with the issuance of Notice 1650.19.

### SECTION 2. RESPONSIBILITIES

**4. IMPLEMENTATION.** Regional and center division/staff managers are responsible for taking appropriate action to ensure that the requirements of this order are met and that FIRS is fully implemented within their respective areas of jurisdiction.

**5. REGIONAL/CENTER FIRS POINT OF CONTACT (POC).** The manager of each region and CASD/staff will designate at least one primary and one alternate POC for FIRS within his/her respective area of jurisdiction to handle requests for

assistance. The Regional CASIS Coordinator shall be made available to assist in matters involving data or technical problems. The FIRS POC is responsible for maintaining the facility identification table.

**6. PERFORMANCE.** FIRS was conceived with the CAS generalist concept in mind. Due to the large number and complexity of FAA facilities, and the limited resources dedicated to physical security, CAS managers shall consider FIRS appropriate for use by all CAS personnel who are responsible for conducting physical inspections of FAA facilities. At major category 1 facilities, a team concept is recommended; whereby, the AIS specialist, personnel, security specialist, and security control point of contact within the Regional Security Division accomplish the module for their particular discipline.

### SECTION 3. TRAINING

**7. COURSES.** The FIRS User Manual is designed to help the new user understand the FIRS process, but it will not completely supplement the benefits that are derived from a training program supervised by experienced personnel. The Facilities Inspection Course 00023 covers the purpose and application of the FIRS software. Managers should ensure that personnel assigned responsibilities for the conduct of physical security inspections attend course 00023 as required training.

**8. DOCUMENTATION.** Operational and procedural requirements for FIRS applications are contained in the FIRS User Manual VS-ASAS-D-3970 dated November 1990. Copies of this publication may be obtained from the ASAS Hotline. Since FIRS is a dynamic program and may occasionally be revised, CAS managers shall ensure that a current copy is maintained.

## SECTION 4. SCHEDULING

**9. INSPECTION SCHEDULES.** The current version of FIRS does not include an adequate scheduling system. Future versions of FIRS will incorporate this feature. Until the feature is available, a manually prepared schedule of inspections shall be developed by each servicing security element (SSE) and submitted to ACO-320 by October 15 for the current fiscal year. This schedule should be in accordance with latest edition of FAA Order 1650.7, Civil Aviation Security Program Guidelines.

**10. CO-LOCATED FACILITIES.** Inspections performed at co-located facilities shall be identified as separate inspections. Each inspection must include a unique facility identifier from the facility identification code.

## SECTION 5. REPORTING

### 11. REQUIREMENTS.

**a. General.** Only FIRS-generated memorandums and reports, approved by the manager of the SSE, shall be submitted to facility managers. These reports will include all applicable findings and recommendations/ requirements for corrective action as reflected in the "Executive Summary" and the "Summary of Requirements" in the FIRS format.

(1) The approved FIRS report shall be forwarded to facility managers, and shall consist, at a minimum, of the following:

(a) Cover Memorandum. The cover memorandum generated from FIRS.

(b) List of program areas covered. Data sheet indicating the program areas covered in the inspection.

(c) Executive Summary.

(d) Summary of Requirements.

(2) A copy of the completed FIRS inspection modules may be submitted to facility managers, if requested. FIRS checklist may be obtained from SSE's.

(3) Upon request from ACO-320, a complete copy of the FIRS inspection for any facility shall be provided. The inspection report will be transmitted to ACO-320 in accordance with provisions of paragraph 15, section 7 of this appendix.

**b. Record Copy of Inspection Reports.** A complete copy of the validated report shall be retained at the region/center as a permanent record in the form of a WordPerfect document on disk. These data will also be used to upload to the mainframe when appropriate. It should be noted that since only extracts from the inspection report will be uploaded to a host computer at the appropriate time, a permanent record of the entire inspection report will have to be maintained in the region/center data base.

## SECTION 6. FOLLOWUP REPORTING PROCEDURES

### 12. FOLLOWUP REPORTING.

**a. General.** When an inspection results in a specific finding for corrective action, the servicing security element will ensure that there is followup action taken. It is recommended that this action be taken by the inspector responsible for the conduct of the original inspection. The purpose of the followup is to provide a decision as to whether or not the corrective action taken by the facility meets the required standards.

**b. Reporting.** Followup data on requirements for corrective action will be entered into the FIRS data base for the facility. This will include the following:

(1) The status of corrective actions taken on all findings and/or requirements specified in the FIRS report should be received from the facility within 60 days.

(2) Verification may be accomplished by means of communication with the facility manager, supplemental inspection, or both.

(3) The FIRS file for the facility will be updated to reflect the status of the corrective actions. This shall be accomplished by adding to and updating the narrative portion of the FIRS report. The original designation of "F" for finding in the specific program areas concerned will not be changed when corrective action(s) is/are accomplished.

(4) Final disposition reports will be uploaded into FIRS when all outstanding findings have been addressed. When corrective actions have been completed, or when it is determined that the facility is not going to take the required/corrective actions specified in the FIRS report, these data will be entered into the FIRS report for the facility which will then become the final disposition report.

## SECTION 7. SECURITY REQUIREMENTS

### 13. PROTECTIVE MARKING/SAFEGUARDING.

FIRS data, disk storage media, copies of reports, supporting notes, and memorandums will be assigned, as a minimum, the protective marking "FOR OFFICIAL USE ONLY." Marking and safeguarding will be accomplished in accordance with the provisions of the latest edition of FAA Orders 1600.15, Control and Protection of "FOR OFFICIAL USE ONLY" Information, and 1600.54, FAA Automated Information Systems Security Handbook.

**14. CLASSIFIED INFORMATION.** Classified information will not be entered into the FIRS system.

### 15. TRANSMISSION.

a. **Electrical.** FIRS data containing information about the security posture of FAA facilities is sensitive, unclassified, and, as such, will not be transmitted over unprotected telecommunications circuits such as telephone or facsimile. FIRS data may be electrically transmitted over circuits protected by an unclassified crypto algorithm approved for the purpose by the National Security Agency (e.g., type 2 STU-III) or by any means approved for the transmission of classified national security information.

b. **Mail and Pouch Mail.** Refer to Chapter 5 for information concerning transmission by these methods.

## SECTION 8. ASSISTANCE

### 16. REQUESTS FOR ASSISTANCE.

a. Questions concerning the content of this appendix should be addressed to ACP-120, FTS 267-9409.

b. Questions concerning technical inadequacies or difficulties encountered with the FIRS program should be addressed through the appropriate region/center CASIS Coordinator and/or to the ASAS Hotline at FTS 736-5020.